DESARROLLO DE UNA APLICACIÓN WEB DE LIBRE USO PARA EL ANÁLISIS Y GESTIÓN DE RIESGOS BASADO EN LA METODOLOGÍA MÁGERIT, CON PRUEBAS EN UN ENTORNO REAL

OMAR SAID BRITO SALAS
ABEL FRANCISCO SIERRA DIAZ

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2017

DESARROLLO DE UNA APLICACIÓN WEB DE LIBRE USO PARA EL ANÁLISIS Y GESTIÓN DE RIESGOS BASADO EN LA METODOLOGÍA MÁGERIT, CON PRUEBAS EN UN ENTORNO REAL

OMAR SAID BRITO SALAS
ABEL FRANCISCO SIERRA DIAZ

Proyecto de grado para optar al título de
Especialista en Seguridad Informática

Directora:
ING. Lorena Ocampo

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2017

Nota de aceptación:

_____
_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá D.C. 6 de octubre de 2017

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE CUADROS

pág.

LISTA DE ANEXOS

RESUMEN

El presente trabajo de grado consiste en presentar una aplicación web que sirve como herramienta para el análisis y la gestión de riesgos informáticos basada MAGERIT, en el cual se expone la metodología usada para el desarrollo completo de la aplicación, los elementos usados para su construcción, el desarrollo de la base de datos y de la interfaz web.

Palabras claves: MAGERIT, análisis y gestión de riesgos informáticos, información, seguridad informática, vulnerabilidad, amenaza, salvaguarda.

INTRODUCCIÓN

La vida del ser humano no sería lo que se entiende de él si no fuera por las tecnologías de la información. Ellos se encuentran en toda área de nuestras vidas privadas y públicas, individuales y grupales, procesando la información que le es ingresada para así obtener resultados, por ejemplo, llamadas por teléfono celular, mensajería instantánea o chat, imágenes y videos, almacenamiento de datos, entre otros. Dicha información y sus resultados son innatamente clasificados y categorizados en varios temas y también en distintas prioridades, a partir de las cuales se tomarán decisiones. Si la situación descrita se extrapola a grupos empresariales, donde la información es un activo relacionado con la ganancia y pérdida de dinero, las decisiones tomadas sobre ellas y sus resultados determinarán el alcance de los objetivos de negocio.

Es por lo anterior que es menester tratar la información de forma completa como un activo muy importante para la supervivencia y el progreso de una empresa. Se debe tener en cuenta todas sus características, incluyendo los riesgos asociados a la materialización de un ataque voluntario o involuntario a vulnerabilidades existentes en las tecnologías de información. Si se analizan las vulnerabilidades y las acciones necesarias para su tratamiento, y si se logran reducir los riesgos a puntos aceptables, la empresa no estará en posición para ser víctima de hurto, cambio o eliminación de datos importantes y sensibles.

Lo anterior se conoce como análisis y gestión de riesgos, para la cual existen múltiples metodologías para su implementación. La metodología escogida es MAGERIT, oriunda de España. Adicionalmente a ser considerada una de las metodologías más prácticas del rubro, también le es dedicada una herramienta para facilitar el procesamiento de datos relacionados al análisis y la gestión de riesgos, la cual es caracterizada por ser de libre uso únicamente para entidades públicas de España y por tener costo para otros que sienten el interés de usarla.

El propósito del presente trabajo de grado consiste en desarrollar una aplicación web de libre uso para el análisis y gestión de riesgos según MAGERIT, la cuál será sometida a pruebas con datos reales. MAGERIT plantea en su teoría dos modos de empleo, cualitativo y cuantitativo, de los cuales en el presente trabajo de grado se escoge el primero de los dos. La motivación detrás del presente proyecto yace en la inconformidad con la oferta actual de herramientas y aplicaciones para el análisis y gestión de riesgos de sistemas de la información ya que no se encuentran aplicaciones que no dependan de una instalación en un computador local y tampoco

de las licencias con precios. Al realizar una aplicación web de libre uso, se eliminan las dos características anteriores, habilitando así su uso para el público y para su mejora continua.

1. JUSTIFICACIÓN

En el mercado de la seguridad de la información yacen multitudes de metodologías de análisis y gestión de riesgos, adaptables y aplicables para todo estilo de organización. Entre ellas se encuentra CORAS (*Construct a Platform for Risk Analysis of Security Critical Systems*), NIST 800-30 (*National Institute of Standards and Technology*), OCTAVE e *IT Grundschutz*, que según la normativa del negocio y cultura del lugar o país en el que se funda o aplica la metodología, existirán semejanzas y/o diferencias entre ellas. La metodología tomada en cuenta en el presente documento es MAGERIT que, en su estructura característica de identificación, clasificación y división de activos de tecnologías de la información de una organización, para luego identificar los riesgos asociados y las contramedidas pertinentes, es entre las más conocidas y aplicadas en el rubro, constando de tres tomos de información para su práctica y multitudes de aplicaciones tecnológicas para su fácil comprensión y ejercicio.

Entre dichas aplicaciones centradas en MAGERIT, no existe alguna de uso libre y gratis. Aún al comprender los motivos por los cuales dichas aplicaciones son pagas, la principal desventaja consiste en la compra de las licencias para usar dicho programa a su máxima potencia. Al desarrollar una aplicación de libre y gratis, el factor económico no será impedimento, habilitando así el empleo de la herramienta sin la preocupación de obtener una versión de prueba con limitadas funciones, sino la obtención de un programa que ayude en el análisis y en la gestión de los riesgos en sistemas de tecnologías de la información con todas las funciones.

A lo anterior se le suma la característica de ser una aplicación en entorno web, que a su vez independiza al usuario de la descarga de la aplicación en mención en computadores individuales y aislados. Dado que el Internet expande su presencia rápidamente a todo rincón de la actividad humana y labor empresarial, usar la aplicación en entorno web ampliaría la disponibilidad de su uso.

2. PROBLEMA DE INVESTIGACIÓN

2.1 PLANTEAMIENTO

Actualmente, el mundo es testigo de múltiples ataques informáticos que comprometen los activos de las compañías vulneradas, como también la información que almacenan. Por ende, el análisis y gestión de riesgos se establece como un requisito importante para revelar los riesgos presentes en el entorno empresarial, para así entender las formas para mitigarlos.

Dado lo anterior, para ello resulta necesario el uso de herramienta para promover la eficiencia y efectividad del análisis y gestión de riesgos. Dichas herramientas vienen en la forma de un programa digital, entre los cuales existen aquellos que requieren un pago y aquellos que es de libre uso. El último trae beneficios en presupuesto, recursos, tiempo y en retorno de la inversión.

No obstante, a pesar de existir software de libre uso, solo existe una oferta completa que se basa en el método MAGERIT, que viene en la forma de un programa, a la cual se le debe activar licencias que permiten su uso completo, todo en un espacio de 30 días.

La creación de una aplicación web de libre uso para el análisis y gestión de riesgos basados en la metodología MAGERIT presenta ventajas necesarias ya que no requiere de una instalación nueva y tampoco de licencias temporales o pagas. Su disponibilidad de uso aumentará y su utilización completa es un factor determinante en la eficiencia de empleo y resultados.

2.2 FORMULACIÓN

¿Qué herramienta basada en la metodología MAGERIT sería útil para ayudar a un usuario o grupo de usuarios en el análisis y gestión de riesgos informáticos, de tal manera que no se incurra en costos por compra de aplicación, licencias y de más honorarios?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

- Desarrollar una aplicación web de libre uso para el análisis y gestión de riesgos basado en la metodología MAGERIT, de modalidad cualitativa, con pruebas en un entorno real.

3.2 OBJETIVOS ESPECÍFICOS

- Levantar los requerimientos necesarios para realizar el diseño de la aplicación web.

- Elegir las herramientas de trabajo para el desarrollo de la aplicación.

- Plasmar en un *Backlog* la pila del producto con las historias de usuario.

- Diseñar el modelo Entidad-Relación entre los diferentes elementos de la metodología.

- Implementar la aplicación con arquitectura web basado en los elementos listados en el *Backlog*.

- Realizar pruebas de escritorio inicialmente sobre la base de datos de la aplicación.

- Realizar pruebas sobre la aplicación web desde la perspectiva de un entorno real, usando datos reales de activos de tecnologías de la información y los riesgos asociados a ellos.

- Documentar el manual de la aplicación web mientras se cumplen con los objetivos establecidos en el *Backlog*.

4. MARCO TEÓRICO

4.1 RIESGO DE SEGURIDAD INFORMÁTICA

La probabilidad de que una amenaza específica logre explotar una vulnerabilidad para causar una pérdida o un daño en un activo de información[1].

4.2 VULNERABILIDAD

La debilidad de un activo o control que tiene el potencial de ser explotado por una o varias amenazas[2].

4.3 ANÁLISIS DE RIESGOS INFORMÁTICOS

Es el proceso que consiste en la identificación de activos informáticos, sus vulnerabilidades y sus amenazas, la probabilidad de materialización del riesgo y el impacto del mismo, para luego determinar los controles adecuados para decidir una o un grupo de las siguientes opciones: reducir, evitar, compartir y aceptar el riesgo completo o residual[3].

4.4 MAGERIT

MAGERIT es el acrónimo de "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" y consiste en una metodología para el análisis y la gestión de riesgos desarrollada por el Consejo Superior de Administración Electrónica CSAE. Dicha metodología es de libre uso público y se puede implementar sin el expreso consentimiento del Ministerio de Administraciones Públicas de España. La versión más actualizada es la tercera y consta de tres libros: Libro I – Método, Libro II – Catálogo de Elementos y Libro III – Guía de Técnicas. El primer libro consiste

[1] EL PORTAL DE ISO 27001 EN ESPAÑOL. Glosario - Riesgo. [en línea]. Disponible en: http://www.iso27000.es/glosario.html.
[2] EL PORTAL DE ISO 27001 EN ESPAÑOL. Glosario - Vulnerabilidad. [en línea]. Disponible en: http://www.iso27000.es/glosario.html.
[3] ANÁLISIS DE RIESGO. Análisis de Riesgos Informáticos. [en línea]. Disponible en: https://es.slideshare.net/JordyMichael26/analisis-de-riesgo-informatico.

en presentar la estructura por medio de la cual se fundamenta el modelo de análisis y gestión de riesgos. El segundo libro expone un inventario de activos y sus clasificaciones, las características importantes para valorar los activos identificados, y adicionalmente un listado de amenazas y controles que se debe tener en consideración. Por último, el tercer libro expone las diferentes técnicas usadas para el análisis y gestión de riesgos, donde se contiene alternativas como análisis con tablas, algoritmos, árboles de ataque, análisis de costo/beneficio, entre otras. Estos tres libros son gratuitos y de libre uso[4].

A continuación, se halla la explicación de cada uno de sus elementos básicos:

- **Activo** – El elemento más importante de la metodología, de la cual se basa todo el análisis y la gestión de riesgos[5]. La aplicación de la metodología se realiza por activo, el cual a su vez se caracteriza por tres elementos fundamentales: el valor, la amenaza y la salvaguarda.

- **Dominio** – Una colección de activos uniformemente protegidos bajo una única autoridad. Todo activo debe estar en algún dominio y cada activo pertenece solo a un dominio[6].

- **Dimensión** – Un aspecto o una característica que se diferencia de otras, respecto del que se puede medir el valor de un activo en función del perjuicio que causaría su pérdida de valor[7].

- **Valor** – La cualidad estimable (en muchos casos, costo/precio) que posee algún bien o activo[8]. El valor se define por las dimensiones de confidencialidad,

[4] WE LIVE SECURITY. MAGERIT: Metodología Práctica para Gestionar Riesgos. [en línea]. Disponible en: https://www.welivesecurity.com/la-es/2013/05/14/MAGERIT-metodologia-practica-para-gestionar-riesgos/

[5] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. Glosario. En: Activo. MAGERIT – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Versión 3.0. Madrid, España, Ministerio de Hacienda y Administraciones Públicas, 2012. Página 97.

[6] AR-TOOLS – Glosario de Términos. [en línea]. Disponible en: http://www.ar-tools.com/es/glossary/index.html.

[7] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. Glosario. En: Dimensión. MAGERIT – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Versión 3.0. Madrid, España, Ministerio de Hacienda y Administraciones Públicas, 2012. Página 100.

[8] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. Glosario. En: Valor. MAGERIT – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Versión 3.0. Madrid, España, Ministerio de Hacienda y Administraciones Públicas, 2012. Página 105.

disponibilidad, integridad, autenticidad y trazabilidad. Adicionalmente, también se define el valor según unos criterios sugeridos por MAGERIT, que se listan a continuación: Despreciable (0), Bajo (1-2), Medio (3-5), Alto (6-8), Muy Alto (9) y Extremo (10).

- **Amenaza** – Causa potencial de un incidente que se traduce en daños a un sistema de información. También se conoce como impacto potencial[9]. MAGERIT sugiere una tabla de elementos predeterminados clasificados en cuatro tipos que serían escogidos por el usuario: de origen natural, de origen industrial, de fallas de aplicación y de origen humano.

- **Salvaguarda –** Procedimiento o mecanismo que reduce el impacto y riesgo que produce una amenaza sobre un activo[10].

- **Degradación –** Pérdida de valor de un activo debido a la materialización de una amenaza[11].

- **Impacto** – La reducción de valor de activo como consecuencia que sobre un activo tiene la materialización de una amenaza. El impacto usualmente se mide con las mismas unidades del valor del activo y es el producto final entre dicho valor y la degradación.

$$Impacto = Valor \times Degradación$$

- **Probabilidad –** La probabilidad de ocurrencia con la que cuenta una amenaza para su materialización completa, que en muchos casos se calcula como ARO (*Annual Rate of Ocurrence*), cuyas unidades consta del número de ocurrencias sobre un año.

---

[9] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. Glosario. En: Activo. MAGERIT – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Versión 3.0. Madrid, España, Ministerio de Hacienda y Administraciones Públicas, 2012. Página 97.

[10] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. Glosario. En: Activo. MAGERIT – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Versión 3.0. Madrid, España, Ministerio de Hacienda y Administraciones Públicas, 2012. Página 103.

[11] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. Glosario. En: Activo. MAGERIT – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Versión 3.0. Madrid, España, Ministerio de Hacienda y Administraciones Públicas, 2012. Página 100.

- **Riesgo** – La estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización[12]. Sus unidades se definen en el valor del activo sobre un año y resulta siendo el producto entre la probabilidad de ocurrencia de la amenaza y el impacto que este ocasiona sobre el activo.

$$Riesgo = Probabilidad \times Impacto$$

- **Eficacia sobre Impacto** – El grado o porcentaje en el cual una salvaguarda reduce la degradación que ocasionaría una amenaza al materializarse sobre un activo.

- **Eficacia sobre Probabilidad** – El grado o porcentaje con el cual una salvaguarda reduce la probabilidad de ocurrencia con la que cuenta una amenaza para materializarse sobre un activo.

- **Degradación Residual –** La degradación remanente luego que una amenaza se materialice sobre un activo que posee alguna salvaguarda. Técnicamente, es el producto entre la degradación y la efectividad de la salvaguarda sobre el impacto.

$$Degradación_{Residual} = Degradación \times (1 - Eficacia_{Impacto})$$

- **Probabilidad Residual –** La probabilidad de ocurrencia remanente luego que una amenaza se materialice sobre un activo que posee alguna salvaguarda. La probabilidad residual es el producto entre la probabilidad de ocurrencia y la efectividad de la salvaguarda sobre la probabilidad.

$$Probabilidad_{Residual} = Probabilidad \times (1 - Eficacia_{Probabilidad})$$

- **Impacto Residual –** El impacto final luego de la materialización de una amenaza sobre un activo que a su vez tiene una salvaguarda que reduce la degradación que

[12] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. Glosario. En: Activo. MAGERIT – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Versión 3.0. Madrid, España, Ministerio de Hacienda y Administraciones Públicas, 2012. Página 102.

potencialmente produciría dicha amenaza sobre un activo. Su resultado se halla como el producto del valor del activo y de la degradación residual.

$$Impacto_{Residual} = Valor \times Degradación_{Residual}$$

- **Riesgo Residual –** El riesgo final luego de la materialización de una amenaza sobre un activo que a su vez tiene una salvaguarda que reduce su probabilidad de ocurrencia. El riesgo residual se halla como el producto del Impacto Residual y de la Probabilidad Residual.

$$Riesgo_{Residual} = Impacto_{Residual} \times Probabilidad_{Residual}$$

4.5 EAR/PILAR

EAR/PILAR (EAR: Entorno de Análisis de Riesgos) es una herramienta desarrollada y financiada parcialmente por el Centro Criptográfico Nacional de España para soportar el análisis y la gestión de riesgos según la metodología MAGERIT. EAR/PILAR cuenta con cuatro versiones con sus distintas variantes y solo son solicitadas por los organismos públicos españoles para obtener licencias libres de cargo. Para todos los demás existe la licencia de evaluación, solo apta para cargar ejemplos previamente compilados por la herramienta[13].

4.6 PLATAFORMA

Una plataforma en términos de la informática consiste en todo soporte de hardware y/o software que usan las aplicaciones en y para su ejecución. Al definir plataformas se establecen los tipos de arquitectura, sistema operativo, lenguaje de programación o interfaz de usuario compatibles[14].

[13] CENTRO CRITPTOLÓGICO NACIONAL. Ear/Pilar. [en línea]. Disponible en: https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar.html.
[14] SAASMANÍA. Diferencia entre Plataforma y Aplicación. [en línea]. Disponible en: http://www.saasmania.com/blog/2008/04/10/diferencia-entre-plataforma-y-aplicacion/.

4.7 MODELO-VISTA-CONTROLADOR

Este es un patrón de arquitectura de software que con los tres componentes de modelo, vista y controlador, separa los datos y la lógica de negocio de una aplicación de la interfaz de usuario y el módulo encargado de gestionar los eventos y las comunicaciones. Es decir, por un lado define componentes para la representación de la información, y por otro lado para la interacción del usuario. Este patrón de arquitectura de software se basa en las ideas de reutilización de código y la separación de conceptos, características que buscan facilitar la tarea de desarrollo de aplicaciones y su posterior mantenimiento.

A continuación, se define cada componente importante de MVC:

- **Modelo** – Esta es la capa donde se trabajan los datos. Entonces, esta capa tendrá mecanismos para acceder a la información y también para actualizar el estado de dicha información, gestionando todos los accesos a dicha información, entre las cuales se involucran las actualizaciones, consultas, búsquedas, entre otras, implementando también los privilegios de acceso que se hayan descrito en las especificaciones de la aplicación. El modelo también se encarga de enviar a la VISTA aquella parte de la información que en cada momento se le solicita para que sea mostrada, normalmente por un usuario. Las peticiones de acceso o manipulación de información llegan al 'modelo' a través del 'controlador'.

- **Controlador** – Contiene el código necesario para responder a las acciones que se solicitan en la aplicación. Su responsabilidad no es manipular la información, pues este es el rol del MODELO, sino que su propósito es de servir como enlace entre el MODELO y la VISTA.

- **Vista** - Presenta el MODELO en un formato adecuado para interactuar con el usuario por tanto requiere de dicho 'modelo' la información que debe representar como salida. Usualmente, en las vistas se usan los códigos HTML y PHP[15].

[15] DESARROLLOWE6. ¿Qué es MVC?. [en línea]. Disponible en: https://desarrolloweb.com/articulos/que-es-mvc.html

4.8 MODELO ENTIDAD-RELACIÓN

Un modelo Entidad-Relación es un tipo de diagrama de flujo que ilustra la relación entre entidades. Estas se usan a menudo para diseñar bases de datos. A continuación, se presentan las definiciones de sus conceptos básicos:

- **Entidad** - La representación de una “cosa”, "objeto" o "concepto" del mundo real con existencia independiente, es decir, se diferencia únicamente de otro objeto o cosa, incluso siendo del mismo tipo, o una misma entidad, por ejemplo, una persona, un automóvil o un puesto de trabajo. Una Entidad esta descrita de características o atributos, por ejemplo, la entidad *Persona* las características: Nombre, Apellido, Género, Estatura, Peso, Fecha de nacimiento.

- **Atributos** - Como mencionado anteriormente, estos son las características que definen o identifican a una entidad. Dentro de los Atributos también existen conceptos básicos que deben ser tomados en consideración.

- *Atributos Identificativos*: son aquellos que permiten diferenciar a una instancia de la entidad de otra distinta, por ejemplo, el número de cédula entre de dos individuos.

- *Dominio*: este hace referencia al tipo de datos que será almacenado para ser tomado por el atributo, entre los cuales se encuentran comúnmente, cadenas de caracteres, números, solo dos letras, solo números mayores que cero, solo números enteros, etc.

- *Valor Nulo*: este se identifica cuando algún atributo correspondiente a una entidad no tiene un valor determinado, bien sea porque no se conoce, porque no existe o porque no se sabe nada al respecto del mismo.

Existe un concepto llamado Correspondencia de Cardinalidades, que dado un conjunto de relaciones en el que participan dos o más conjuntos de entidades, la correspondencia de cardinalidad indica el número de entidades con las que puede estar relacionada una entidad dada. Entonces, dado un conjunto de relaciones binarias y los conjuntos de entidades A y B, la correspondencia de cardinalidades puede ser:

- **Uno a Uno** - (1:1) Un registro de una entidad A se relaciona con solo un registro en una entidad B.

- **Uno a Varios** - (1:N) Un registro en una entidad en A se relaciona con cero o muchos registros en una entidad B. Pero los registros de B solamente se relacionan con un registro en A.

- **Varios a Uno** - (N:1) Una entidad en A se relaciona exclusivamente con una entidad en B. Pero una entidad en B se puede relacionar con 0 o muchas entidades en A.

- **Varios a Varios** - (N:M) Una entidad en A se puede relacionar con 0 o con muchas entidades en B y viceversa[16].

4.9 SCRUM

SCRUM es el nombre con el que se denomina a los marcos de desarrollo ágiles caracterizados por:

- Adoptar una estrategia de desarrollo incremental, en lugar de la planificación y ejecución completa del producto.

- Basar la calidad del resultado más en el conocimiento tácito de las personas en equipos auto organizados, que en la calidad de los procesos empleados.

- Solapamiento de las diferentes fases del desarrollo, en lugar de realizar una tras otra en un ciclo secuencial o en cascada.

Entre las características generales de SCRUM se encuentran los roles: el SCRUM Master, el *Product Owner*, y el Team (equipo) que ejecuta el desarrollo y demás elementos relacionados con él. Durante cada Sprint (un periodo entre una y cuatro semanas) el equipo crea un incremento de software potencialmente entregable.

[16] LUCIDCHART. ¿Qué es un Diagrama Entidad-Relación?. [en línea]. Disponible en: https://www.lucidchart.com/pages/es/qu%C3%A9-es-un-diagrama-entidad-relaci%C3%B3n

El conjunto de características que forma parte de cada sprint viene del *Product Backlog*, cuyos elementos se determinan durante la reunión de *Sprint Planning*. Durante esta reunión, el *Product Owner* identifica los elementos del *Product Backlog* que quiere ver completados. Entonces, el equipo conversa con el *Product Owner* buscando la claridad y magnitud adecuadas para luego determinar la cantidad de ese trabajo que puede comprometerse a completar durante el siguiente *Sprint*. Durante el *Sprint*, nadie puede cambiar el *Sprint Backlog*, lo que significa que los requisitos están congelados durante el *Sprint*.

Existen varias implementaciones de sistemas para gestionar el proceso de SCRUM, que van desde notas amarillas *post-it* y pizarras hasta paquetes de software. No obstante, en cualquiera de sus metodologías cualquier miembro del equipo podrá ver tres columnas: trabajo pendiente ("*Backlog*"), tareas en proceso ("*In Progress*") y hecho ("*Done*"). De un solo vistazo, una persona puede ver en qué están trabajando los demás en un momento determinado.

A continuación, se definen los roles:

- **Product Owner** - Se asegura de que el equipo SCRUM trabaje de forma adecuada desde la perspectiva del negocio. El *Product Owner* escribe historias de usuario, las prioriza, y las coloca en el *Product Backlog*.

- **SCRUM Master (o Facilitador)** - El SCRUM es facilitado por un *SCRUM Master*, cuyo trabajo primario es eliminar los obstáculos que impiden que el equipo alcance el objetivo del Sprint así asegurando que el proceso SCRUM se utiliza como es debido. El SCRUM Master es el que hace que las reglas se cumplan.

- **Equipo SCRUM** - El equipo tiene la responsabilidad de entregar el producto. Es recomendable un pequeño equipo de 5 a 9 personas con las habilidades transversales necesarias para realizar el trabajo.

Para el correcto seguimiento de las tareas diarias, cada día de un Sprint, se realiza la ceremonia sobre el estado de un proyecto. Esto se llama *Daily Standup* o *Stand-up Meeting*. SCRUM tiene unas guías específicas:

- La ceremonia comienza puntualmente a su hora.

- Todos son bienvenidos, pero sólo los involucrados en el proyecto pueden hablar.

- La ceremonia tiene una duración máxima de 15 minutos, de forma independiente del tamaño del equipo.

- La ceremonia debe celebrarse idealmente en la misma ubicación y a la misma hora todos los días.

Durante la ceremonia, cada miembro del equipo contesta a tres preguntas:

- ¿Qué has hecho desde ayer?

- ¿Qué es lo que haré hoy?

- ¿Has tenido algún problema que te haya impedido alcanzar tu objetivo? (Es el papel del SCRUM Master recordar estos impedimentos).

La meta principal de las ceremonias diarias es que cada miembro del equipo sepa si se están cumpliendo los plazos marcados para el *Sprint*.

A continuación, se definen los documentos primordiales que deben ser formados durante el SCRUM:

- **Product Backlog** - Esto trata de un documento de alto nivel para todo el proyecto. Es el conjunto de todos los requisitos de proyecto, el cual contiene descripciones genéricas de funcionalidades deseables, priorizadas según su retorno sobre la inversión (ROI). Representa el qué va a ser construido en su totalidad. Es abierto y solo puede ser modificado por el *Product Owner*. Contiene estimaciones realizadas a grandes rasgos, tanto del valor para el negocio, como del esfuerzo de desarrollo requerido. Esta estimación ayuda al *Product Owner* a ajustar la línea temporal (KEV) y, de manera limitada, la prioridad de las diferentes tareas. Por ejemplo, si dos características tienen el mismo valor de negocio la que requiera menor tiempo de desarrollo tendrá probablemente más prioridad, debido a que su ROI será más alto.

- **Sprint Backlog** - Este es el subconjunto de requisitos que serán desarrollados durante el siguiente *Sprint*. Al definir el *sprint Backlog*, se describe el cómo el equipo va a implementar los requisitos durante el Sprint. Por lo general los requisitos se subdividen en tareas, a las cuales se asignan ciertas horas de trabajo, pero ninguna tarea con una duración superior a 16 horas. Si una tarea es mayor de 16 horas, deberá ser dividida en otras menores. Las tareas en el *sprint Backlog* nunca son asignadas, son tomadas por los miembros del equipo del modo que les parezca adecuado.

- **Burn Down Chart** - Es una gráfica mostrada públicamente que mide la cantidad de requisitos en el *Backlog* del proyecto pendientes al comienzo de cada *Sprint*. Dibujando una línea que conecte los puntos de todos los *Sprints* completados, podremos ver el progreso del proyecto. Lo normal es que esta línea sea descendente (en casos en que todo va bien en el sentido de que los requisitos están bien definidos desde el principio y no varían nunca) hasta llegar al eje horizontal, momento en el cual el proyecto se ha terminado (no hay más requisitos pendientes de ser completados en el *Backlog*). Si durante el proceso se añaden nuevos requisitos la recta tendrá pendiente ascendente en determinados segmentos, y si se modifican algunos requisitos la pendiente variará o incluso valdrá cero en algunos tramos[17].

4.10 PHP

PHP es un acrónimo para *Hypertext Preprocessor*, lo cual consiste en un lenguaje de código abierto bastante usado para el desarrollo de páginas web. Entre sus ventajas existe el poder ser incrustado en el lenguaje HTML, tal que el usuario final que observa la página nunca sabrá el código PHP subyacente. Finalmente, PHP es un código ejecutado en el servidor.

4.11 MYSQL

MySQL es un sistema de gestión de bases de datos relacional desarrollado bajo la licencia dual GPL/Licencia comercial Oracle Corporation y está considerada como la base datos open source más popular del mundo. Este es originalmente escrito en C/C++ y es reconocido por su gran adaptación a diferentes entornos de desarrollo, así permitiendo su interacción con diferentes lenguajes de programación.

[17] VIDEO2BRAIN. Aprende SCRUM. [en línea]. Disponible en: https://www.handybackup.net/backup_terms/phpmyadmin-definition.shtml

MySQL es patrocinado por una empresa privada, que posee los derechos de autor de la mayor parte del código. Esto es lo que posibilita el esquema de doble licenciamiento anteriormente mencionado. La base de datos se distribuye en dos versiones principales:

- *Community*, distribuida bajo la Licencia pública general de GNU, versión 2.

- Enterprise, para aquellas empresas que quieran incorporarlo en productos privados. Las versiones Enterprise incluyen productos o servicios adicionales tales como herramientas de monitorización y soporte oficial.

Adicionalmente, hay tres tipos de compilación del servidor MySQL:

- **Estándar** - Los binarios estándares de MySQL son los recomendados para la mayoría de los usuarios, e incluyen el motor de almacenamiento InnoDB.

- **Max** - Los binarios incluyen características adicionales que no han sido lo bastante probadas o que normalmente no son necesarias.

- **MySQL-Debug** - Son binarios que han sido compilados con información de depuración extra. No debe ser usada en sistemas en producción porque el código de depuración puede reducir el rendimiento[18].

4.12 DESARROLLO ÁGIL DE SOFTWARE

El desarrollo ágil de software es, como respuesta contra el método en cascada, una metodología en la que el desarrollador va adaptando sus soluciones a unos requisitos cambiantes a lo largo del tiempo. Así el trabajo es realizado mediante la colaboración de equipos auto-organizados y multidisciplinarios, inmersos en un proceso compartido de toma de decisiones a corto plazo.

[18] ESEPE STUDIO ESPECIALISTAS 10.0. ¿Qué es MySQL?. [en línea]. Disponible en: http://www.esepestudio.com/noticias/que-es-mysql

Cada iteración del ciclo de vida incluye: planificación, análisis de requisitos, diseño, codificación, pruebas y documentación. En cada iteración, el equipo de desarrollo no tiene la obligación de entregar todo el programa sino de entregar pequeños elementos probados, sin errores, con el fin de entregar una solución final totalmente operativa. Para ellos, la comunicación entre los miembros del equipo es importante.

Es importante aclarar que los métodos ágiles hacen énfasis en las comunicaciones cara-a-cara en vez de la documentación. Los métodos ágiles también se concentran en que el software funcional es la primera medida del progreso.

Para que una metodología de desarrollo de software se pueda considerar como ágil, se debe cumplir con cuatro valores fundamentales:

- Los individuos e interacciones, por encima de los procesos y herramientas.
- Software en funcionamiento, por encima de la documentación exhaustiva.
- La colaboración con el cliente, por encima de la negociación contractual.
- La respuesta al cambio, por encima del seguimiento de un plan.

A continuación, se presentan algunos métodos ágiles de desarrollo de software:

- Adaptive Software Development (ASD)
- Agile Unified Process
- Crystal Clear
- Feature Driven Development (FDD)

- Lean Software Development (LSD)
- Kanban (desarrollo)
- Open Unified Process (OpenUP)
- Programación Extrema (XP)
- Método de desarrollo de sistemas dinámicos (DSDM)
- SCRUM
- 6D-BUM[19]

4.13 LARAVEL

Este un marco de código abierto creado por Taylor Otwell en el año 2011 para desarrollar aplicaciones y servicios web en lenguaje PHP basado en la arquitectura MVC, y es relativamente nuevo en el mercado de marcos de código en comparación de *Ruby on Rails* y *Django* de *Python*. Su filosofía es facilitar el desarrollo par artistas web, proporcionando una forma de codificación elegante y simple, y permitir multitud de funcionalidades. Intenta aprovechar lo mejor de otros marcos y aprovechar las características de las últimas versiones de PHP[20].

[19] TICBEAT. ¿Qué es el desarrollo ágil y cómo está transformando la industria del software?. [en línea]. Disponible en: http://www.ticbeat.com/tecnologias/que-es-el-desarrollo-agil-y-como-esta-transformando-la-industria-del-software/

[20] LYNDA. What is Laravel?. [en línea]. Disponible en: https://www.lynda.com/Laravel-tutorials/What-Laravel/604257/648635-4.html

4.14 PHPMYADMIN

Este es un software libre uso escrito en PHP y provee una interfaz gráfica conveniente para el trabajo en DBMS de MySQL. Como referencia completa de uso, existe un libro escrito por uno de los desarrolladores de phpMyAdmin llamado *Mastering phpMyAdmin for Effective MySQL Management*[21].

4.15 XAMPP

XAMPP es una distribución libre de Apache que contiene MariaDB, PHP y Perl[22].

[21] HANDY BACKUP. phpMyAdmin Definition. [en línea]. Disponible en: https://www.handybackup.net/backup_terms/phpmyadmin-definition.shtml

[22] APACHE FRIENDS. Xampp Apache+MariaDB+PHP+Perl. [en línea]- Disponible en: https://www.apachefriends.org/es/index.html

5. DISEÑO METODOLÓGICO

Esta sección revela el procedimiento organizado con el que se afrontó el presente proyecto, tomando en cuenta el planteamiento de cada uno de los objetivos específicos. El diseño metodológico y en efecto los objetivos específicos se dividen en tres grupos de metas: los requerimientos iniciales, el desarrollo de la base de datos y el desarrollo de la aplicación web. La sección de requerimientos iniciales muestra el levantamiento de la información y condiciones previas al desarrollo de la aplicación web y las herramientas que fueron usadas para su implementación. Luego, en la sección del desarrollo de la base de datos se expone el modelo Entidad-Relación construido a partir de los elementos y fundamentos básicos de MAGERIT. Finalmente se revela el producto final de la aplicación web, evidenciando así su funcionamiento y su estructura mediante un ejemplo.

5.1 LEVANTAMIENTO DE REQUERIMIENTOS

Antes de contemplar el desarrollo de la aplicación web, era necesario entender los requerimientos fundamentales a partir de los cuales se hará la construcción del proyecto. Hubo tres necesidades primordiales a ser considerados previos al desarrollo: la obtención de datos y variables para su uso en las pruebas del funcionamiento del producto final, el entendimiento de la propuesta de MAGERIT para su posterior inclusión en la aplicación y finalmente, las historias de uso.

Inicialmente, se consultaron los dos libros finales de la propuesta MAGERIT para entender técnicamente los elementos básicos de la aplicación web. Primeramente, en el Libro II – Catálogo de Elementos de MAGERIT se encuentra una lista de categorías y elementos que funcionan como referencia contra la cual aquella persona o empresa que desea emprender el análisis y gestión de riesgos de sistemas de la información puede basarse para la apropiada clasificación de los activos, sus amenazas y sus salvaguardas. Existen elementos para los activos, las amenazas y las salvaguardas, que MAGERIT organiza y nombra en categorías fundamentales, junto con un código identificador por elemento. Dichos catálogos fueron usados como datos prestablecidos para la construcción de la base de datos y funcionaron como factores en los cálculos de impacto, riesgo y otras variables asociadas.

Libro III – Guía de Técnicas fue el otro libro de MAGERIT consultado para entender el propósito y la relación o interacción entre los elementos básicos del análisis y gestión de riesgos de sistemas de información. Aquí MAGERIT presenta los

elementos que deben ser escogidos por el usuario y las fórmulas o procedimientos para obtener los resultados del impacto, riesgo y las variables residuales, cuya síntesis fue plasmada en el marco teórico del presente documento.

Luego, se considera la obtención de datos desde un entorno real para la verídica validación del funcionamiento de la versión final de la aplicación. Estos fueron obtenidos gracias a la colaboración de la empresa Constructora IACA y CIA Ltda. previo al desarrollo de la base de datos y de la aplicación web. La empresa en mención no solo proporcionó datos de los activos que considera importantes dentro de la compañía, sino que también, luego de una capacitación básica en torno a la valoración de activos, degradación de la valoración, probabilidad de ocurrencia de amenazas y las eficacias de las salvaguardas, proporcionó la información restante útil para hacer las pruebas. Finalmente, dichos datos fueron registrados en tablas encontradas en Cuadro 1, Cuadro 2, Cuadro 3 y Cuadro 4.

Cuadro 1. Información de Activos

Información de Activos					
ID	**Tipo de Activo**	**Nombre de Activo**	**Propietario del Activo**	**Descripción de Activo**	**Actividad del Activo**
1	HW.pc	Computador Portátil	Constructora IACA	Lenovo 8gb RAM Core i5 1TB Disco Duro	Ofimática, Modelado de Planos
2	HW.print, HW.scan	Impresora Multifuncional	Constructora IACA	HP LaserJet Pro 200 color MFP	Impresiones, Escaneo, Fotocopias
3	COM.Internet	Internet Corporativo	Constructora IACA	Router Arris TG862	Conectividad a Internet, Comunicación LAN
4	Media.printed	Archivador	Constructora IACA	Archivador Metálico de 3 puestos	Archivar documentos físicos
5	Media.usb	Memoria USB	Constructora IACA	Memorias para el trabajo diario	Archivar documentos digitales
6	Media.disk	Disco Duro Portátil	Constructora IACA	Western Digital 1TB	Archivar documentos digitales para mayor capacidad

Omar Brito y Abel Sierra.

Cuadro 2. Información de Amenazas

Información de Amenazas				
ID	**Tipo de Amenaza**	**Nombre de Amenaza**	**Descripción de Amenaza**	**Activo Amenazado**
1	A.25	Hurto de Máquina	Degradación de Hardware	Computador Portátil
2	I.5	Daño de Equipo	Frecuencia de Avería de Máquina	Impresora Multifuncional
3	E.24	Saturación de BW	Degradación de Uso de BW de la Compañía	Internet Corporativo
4	A.6	Acceso a Archivos Físicos	Degradación de Confidencialidad de Información	Archivador
5	E.25	Pérdida de Memoria	Degradación de Confidencialidad de Información	Memoria USB
6	A.15	Cambios en los Archivos	Degradación de Integridad de Datos	Disco Duro Portátil

Omar Brito y Abel Sierra.

Cuadro 3. Información de Salvaguardas

Información de Salvaguardas					
ID	**Tipo de Salvaguarda**	**Nombre de Salvaguarda**	**Descripción de Salvaguarda**	**Activo a Proteger**	**Amenaza Que Mitigar**
1	HW	Guaya	Guaya para el Computador Portátil	Computador Portátil	Hurto de Máquina
2	AUX.AC	Ventilación	Cambio de Ubicación de la Impresora donde reciba mejor Ventilación	Impresora Multifuncional	Daño de Equipo
3	COM.Internet	Filtros de Navegación	Permisos/Prohibiciones por Control de Contenido Web	Internet Corporativo	Saturación de BW
4	L.AC	Seguridad Física	Cambio de Ubicación donde se use una Puerta con Seguridad para Acceso	Archivador	Acceso a Archivos Físicos
5	PS.AT	Educación a Personal	Educación al Personal de Trabajo en conocimientos de Seguridad de la Información	Memoria USB	Pérdida de Memoria
6	H.AU	HIDS	Control de Cambios de Archivos	Disco Duro Portátil	Cambios en los Archivos

Omar Brito y Abel Sierra.

Cuadro 4. Información de Datos

Información de Datos						
	Valoración		Propiedades de la Amenaza		Propiedades de Salvaguarda	
ID	Dimensión	Valor	Nivel de Degradación	Nivel de Probabilidad	Eficacia/Impacto	Eficacia/Probabilidad
1	Disponibilidad	9	100%	0,1	80%	100%
2	Disponibilidad	5	30%	4	90%	50%
3	Disponibilidad	8	80%	20	30%	30%
4	Confidencialidad	8	25%	2	90%	90%
5	Confidencialidad	3	10%	0,5	60%	20%
6	Integridad	7	80%	0,4	70%	0%

Omar Brito y Abel Sierra.

La tabla de activos lista los recursos que la empresa Constructora IACA y CIA Ltda. consideró en poseer la capacidad de almacenar, procesar y efectuar cambios en la información. A su vez, la empresa también plasmó una calificación cualitativa para asociarle una valorización a cada activo. La tabla de amenazas lista aquellas que vulnerarían los activos registrados, junto con la degradación y la probabilidad de ocurrencia de cada amenaza. Finalmente, la tabla de salvaguardas contiene una lista de aquellas que mitigan tanto el impacto como la probabilidad de ocurrencia de las amenazas previamente mencionadas, en la cual Constructora IACA y CIA Ltda. aportó lo que considera ser los valores de la eficacia sobre el impacto y la eficacia sobre la probabilidad.

Finalmente, se plasman las historias de uso, que en esencia consisten en requisitos puntuales necesarios para el desarrollo aplicación web basada en MAGERIT. Estas son registradas en el *Backlog* en un lenguaje común, y son listadas a continuación:

- Realizar el levantamiento de la información.
- Diseñar el modelo de datos de la aplicación.
- Crear el modelo vista-controlador del modelo resultante.
- Escoger plantilla *Bootstrap* para la interfaz gráfica de la aplicación.

Adicionalmente, la aplicación debe tener las siguientes características:

- Ofrecer a los usuarios la gestión de los datos básicos de un proyecto.
- Ofrecer a los usuarios escoger y agregar activos del catálogo al proyecto.
- Ofrecer a los usuarios la selección de las posibles amenazas que potencialmente vulneran los activos.
- Ofrecer a los usuarios el ingreso de la valoración cualitativa de los activos.

- Ofrecer a los usuarios la selección de las posibles salvaguardas contra las amenazas escogidas.

- Ofrecer al usuario la posibilidad de ingresar valores de degradación, probabilidad de ocurrencia de una amenaza y las eficacias de las salvaguardas.

- Ofrecer al usuario un manual de uso de la aplicación.

- Ofrecer al usuario el cálculo automático del impacto, del riesgo, de la degradación residual, de la probabilidad residual, del impacto residual y del riesgo residual.

- Ofrecer al usuario la generación automática de un reporte de resultados.

5.2 ELECCIÓN DE HERRAMIENTAS

Para el cumplimiento de las condiciones desde las cuales se desarrolla el presente proyecto, se elige software libre como herramientas a través de las cuales se desarrollaría la aplicación web de libre uso y estas herramientas son PHP, HTML y MySQL. Estas fueron escogidas por el nivel de experiencia tanto a nivel académico como a nivel profesional que tienen los autores del presente proyecto. Son herramientas versátiles y de simple interpretación. Finalmente, los *frameworks* usados fueron Laravel (HMTL, PHP) para estructurar la aplicación web en mención y phpMyAdmin (SQL, PHP).

5.3 CREACIÓN DEL BACKLOG CON LAS HISTORIAS DE USO

Con el propósito de realizar un desarrollo eficiente y organizado, teniendo en consideración los percances y las fallas que pueden aparecer en las etapas del desarrollo y a su vez en el que los eventuales cambios en etapas anteriores no afecten el tiempo de producción y de entrega final de semejante proyecto, se escoge aplicar SCRUM. Con SCRUM, todas las etapas del desarrollo de la aplicación web lograrán progresar en paralelo, en el caso que correcciones deben hacerse para la mejoría del producto final. Debido a lo anterior, se crea un *Backlog* dentro de la cual se ingresan los puntos expuestos en las historias de uso. Adicionalmente, en el acto

de cumplir con los tres roles fundamentales de SCRUM, los dos integrantes del presente proyecto asumen las siguientes responsabilidades:

Responsabilidades de Omar Brito.

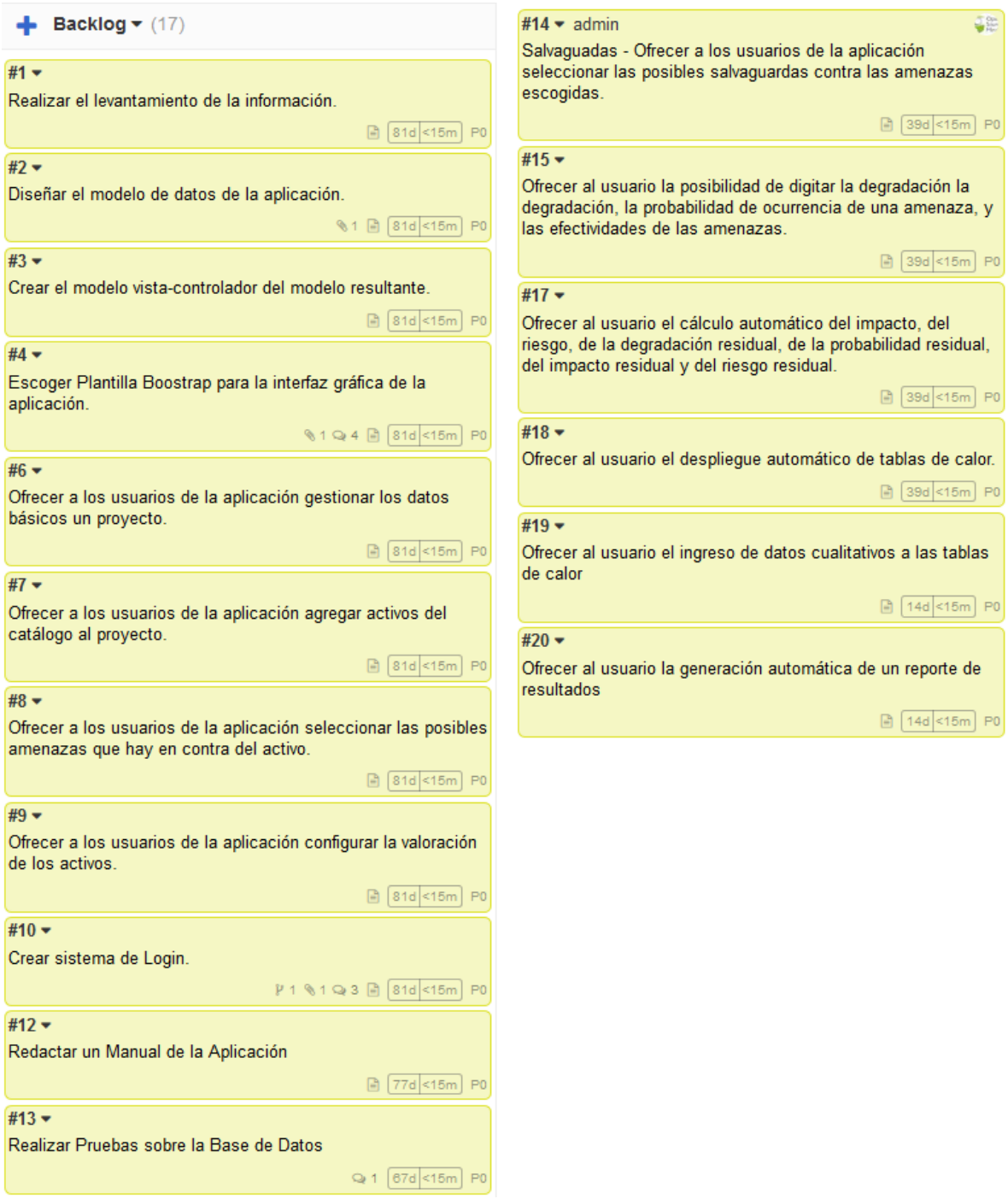
- Trabajo escrito final y artículo IEEE.
- Documentación de las reuniones SCRUM.
- Interpretación y construcción de los algoritmos iniciales según MAGERIT.
- Diseño de la base de datos y aplicación web.
- Pruebas de la base de datos y aplicación web.

Responsabilidades de Abel Sierra.

- Interpretación y construcción de los algoritmos iniciales según MAGERIT.
- Diseño de la base de datos y aplicación web.
- Desarrollo de la base de datos y aplicación web.
- Pruebas de la base de datos y aplicación web.

El primer paso realizado consiste en ingresar las historias de uso, que fueron listadas anteriormente en el documento, en un *Backlog*, la cual es visualizada en Figura 1.

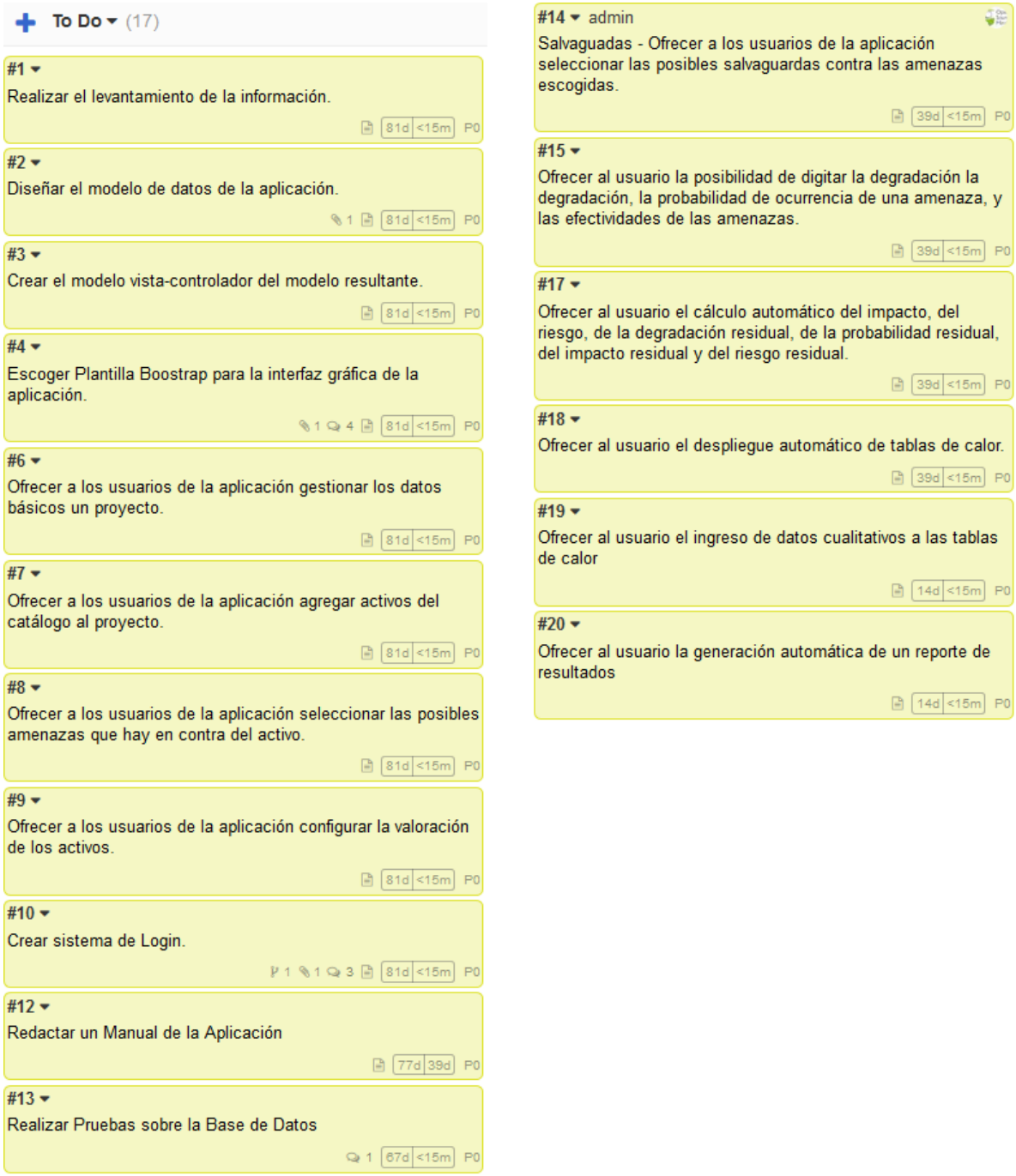
Figura 1. Elementos del *backlog*



Omar Brito y Abel Sierra.

El modo de uso del presente *Backlog* consiste en organizar los elementos en las columnas *To Do*, *In Progress*, *To Test* y *Ready*. En la columna To Do se colocan los elementos que están pendientes por comenzar. En la columna *In Progress* se colocan los elementos que están siendo desarrollados actualmente. To Test es una columna cuyos elementos son aquellos que fueron desarrollados, pero necesitan ser sometidos bajo prueba. *Ready*, finalmente, es una columna cuyos elementos son aquellos que superaron las etapas de desarrollo y pruebas. A continuación, la imagen en Figura 2 ilustra la distribución de dichos elementos en las etapas de inicialización del proyecto.

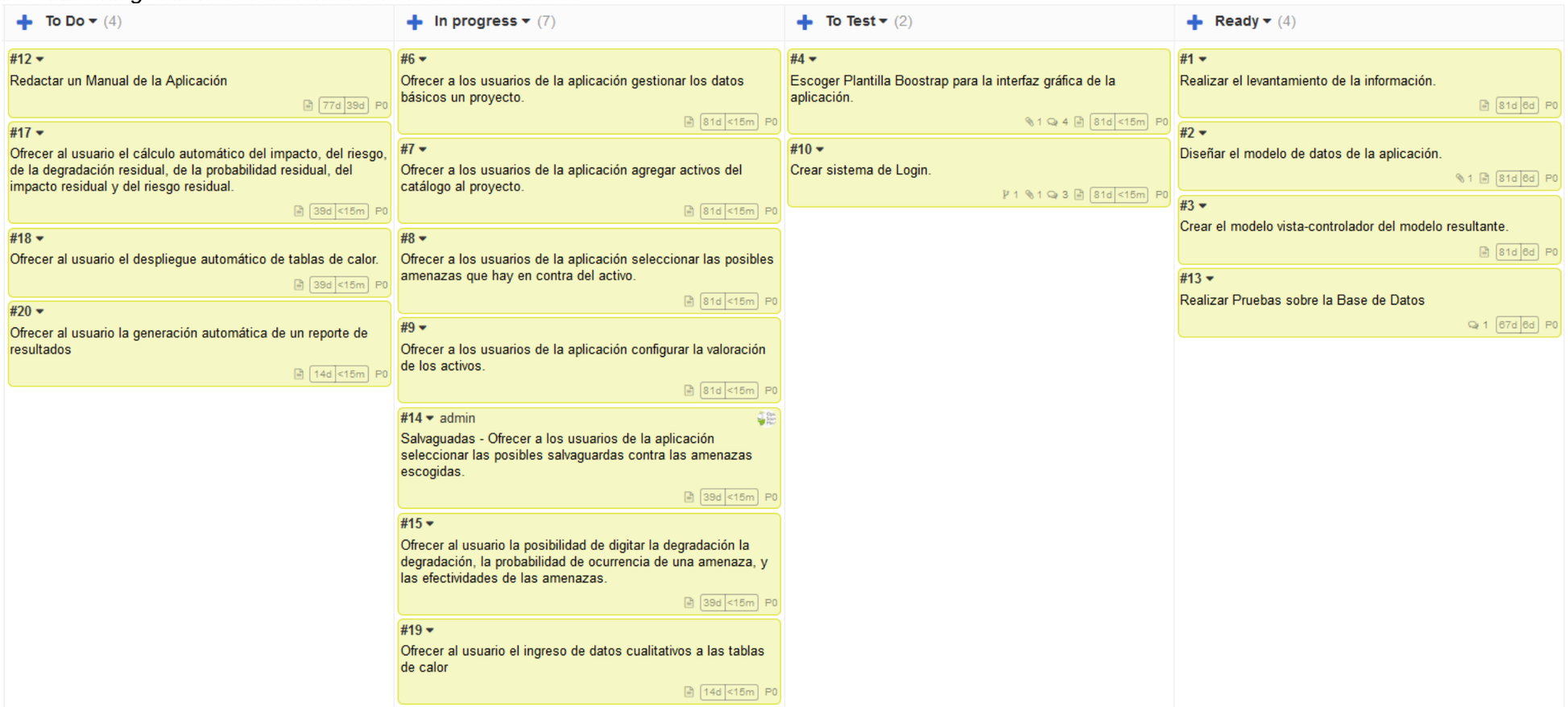
Figura 2. *Backlog* al iniciar el proyecto



Omar Brito y Abel Sierra.

La Figura 3 ilustra la etapa de desarrollo de la base de datos con los diferentes elementos distribuidos según su realización.

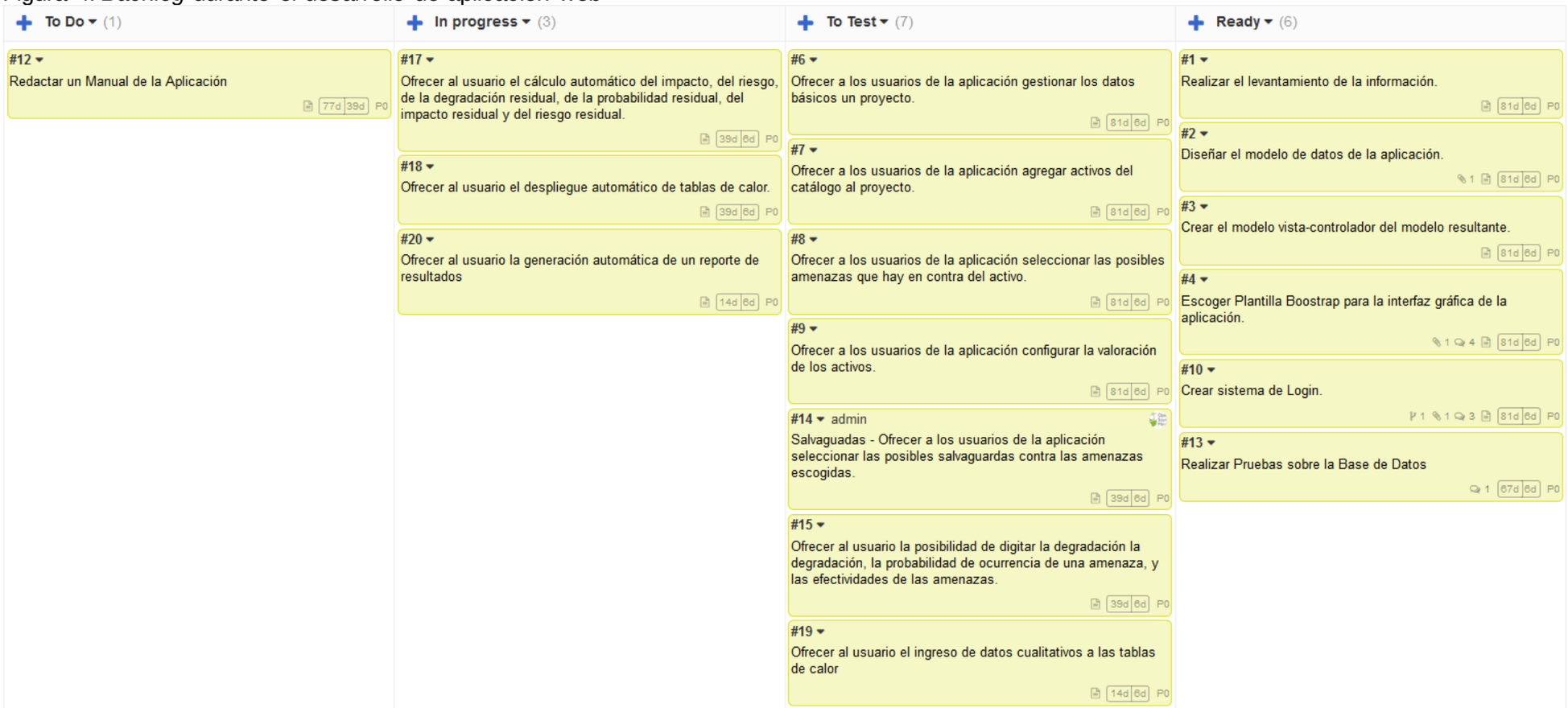
Figura 3. *Backlog* durante el desarrollo de la base de datos



Omar Brito y Abel Sierra.

Finalmente, la Figura 4 ilustra la distribución de los mismos elementos en la etapa del desarrollo de la aplicación web. En ninguna de estas fases hubo la inserción de un nuevo elemento de historia de uso.

Figura 4. *Backlog* durante el desarrollo de aplicación web



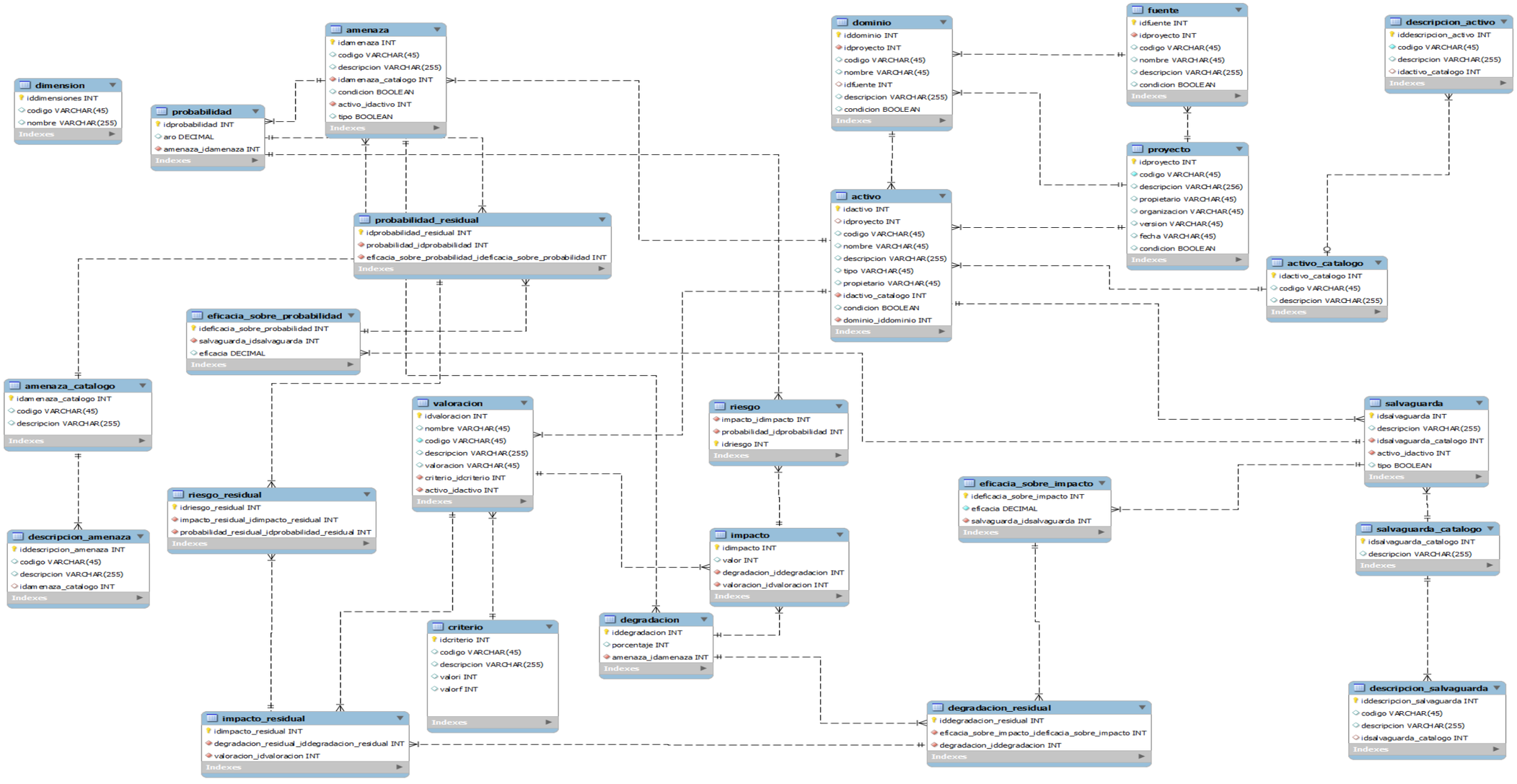
Omar Brito y Abel Sierra.

5.3.1 Reuniones SCRUM. En SCRUM también existe una metodología para organizar las reuniones. Dichas reuniones son útiles para saber en qué estado va el proyecto y qué falta seguir haciendo hasta completar su desarrollo e implementación. Dadas las condiciones personales, espaciales y temporales de los integrantes del proyecto, se adaptaron las fechas de las reuniones según solicitud y demanda de los integrantes, la cuales comprendían ser reuniones presenciales en la Universidad Piloto de Colombia y también reuniones en línea usando Skype, WhatsApp y Gmail. Básicamente, en estas reuniones se discutían preguntas orientadas a la labor que se hizo hasta el momento de la reunión y las labores que se harán a continuación. El registro de las reuniones se encuentra en ANEXO A.

5.4 IMPLEMENTACIÓN DE LA BASE DE DATOS

La base de datos es construida con base al modelo Entidad-Relación, en el que se escogen elementos básicos de MAGERIT que cumplen con la función de Entidad y se construyen las relaciones entre ellas que cumplen con la función de Relación. Cada entidad es a su vez definida por atributos que lo describen, entre los cuales el más importante es el identificador (ID) ya que funciona como elemento de referencia para el llamado de entidades dentro de otras. A continuación, se describe la implementación final de la base de datos, junto con las imágenes que demuestran los valores ingresados en cada atributo para realizar las pruebas con datos reales. El resultante modelo Entidad-Relación se visualiza en la Figura 5, cuya construcción en términos del lenguaje SQL sirve para el desarrollo de la base de datos.

Figura 5. Diagrama entidad-relación



Omar Brito y Abel Sierra.

El siguiente esquema, la Figura 6, de base de datos construido en phpMyAdmin materializa el modelo Entidad-Relación de la imagen anterior, donde cada entidad es representada en un elemento del menú principal.

Figura 6. Tabla de entidades en la base de datos

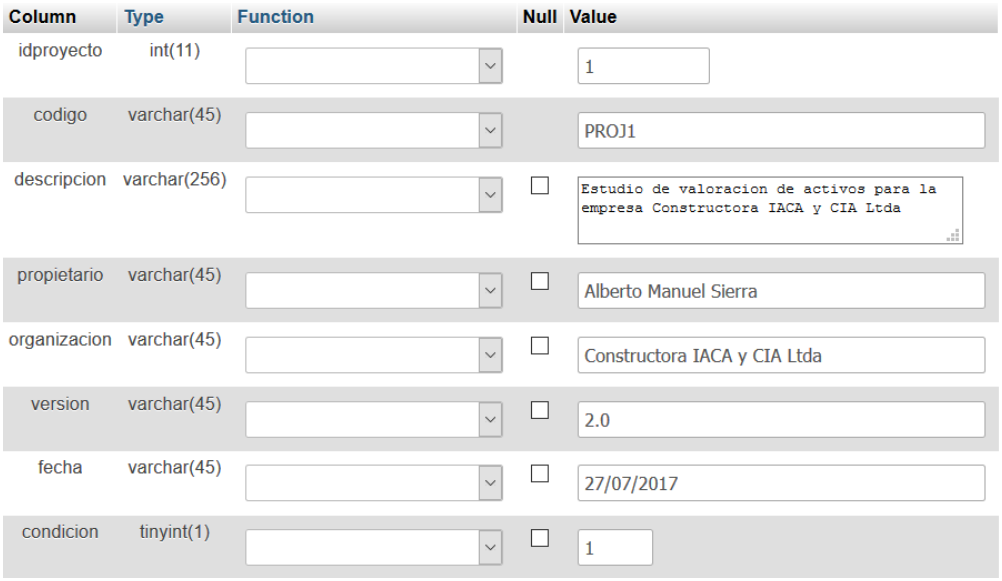
	Table	Action	Rows	Type	Collation	Size	Overhead
☐	activo	Browse Structure Search Insert Empty Drop	1	InnoDB	latin1_swedish_ci	64 KiB	-
☐	activo_catalogo	Browse Structure Search Insert Empty Drop	12	InnoDB	latin1_swedish_ci	16 KiB	-
☐	amenaza	Browse Structure Search Insert Empty Drop	1	InnoDB	latin1_swedish_ci	48 KiB	-
☐	amenaza_catalogo	Browse Structure Search Insert Empty Drop	4	InnoDB	latin1_swedish_ci	16 KiB	-
☐	criterio	Browse Structure Search Insert Empty Drop	6	InnoDB	latin1_swedish_ci	16 KiB	-
☐	degradacion	Browse Structure Search Insert Empty Drop	1	InnoDB	latin1_swedish_ci	32 KiB	-
☐	degradacion_residual	Browse Structure Search Insert Empty Drop	1	InnoDB	latin1_swedish_ci	48 KiB	-
☐	descripcion_activo	Browse Structure Search Insert Empty Drop	91	InnoDB	latin1_swedish_ci	32 KiB	-
☐	descripcion_amenaza	Browse Structure Search Insert Empty Drop	56	InnoDB	latin1_swedish_ci	32 KiB	-
☐	descripcion_salvaguarda	Browse Structure Search Insert Empty Drop	114	InnoDB	latin1_swedish_ci	32 KiB	-
☐	dimension	Browse Structure Search Insert Empty Drop	6	InnoDB	latin1_swedish_ci	16 KiB	-
☐	dominio	Browse Structure Search Insert Empty Drop	5	InnoDB	latin1_swedish_ci	48 KiB	-
☐	eficacia_sobre_impacto	Browse Structure Search Insert Empty Drop	1	InnoDB	latin1_swedish_ci	32 KiB	-
☐	eficacia_sobre_probabilidad	Browse Structure Search Insert Empty Drop	1	InnoDB	latin1_swedish_ci	32 KiB	-
☐	fuente	Browse Structure Search Insert Empty Drop	5	InnoDB	latin1_swedish_ci	32 KiB	-
☐	impacto	Browse Structure Search Insert Empty Drop	1	InnoDB	latin1_swedish_ci	16 KiB	-
☐	impacto_residual	Browse Structure Search Insert Empty Drop	1	InnoDB	latin1_swedish_ci	48 KiB	-
☐	probabilidad	Browse Structure Search Insert Empty Drop	1	InnoDB	latin1_swedish_ci	16 KiB	-
☐	probabilidad_residual	Browse Structure Search Insert Empty Drop	1	InnoDB	latin1_swedish_ci	48 KiB	-
☐	proyecto	Browse Structure Search Insert Empty Drop	1	InnoDB	latin1_swedish_ci	16 KiB	-
☐	riesgo	Browse Structure Search Insert Empty Drop	1	InnoDB	latin1_swedish_ci	48 KiB	-
☐	riesgo_residual	Browse Structure Search Insert Empty Drop	1	InnoDB	latin1_swedish_ci	48 KiB	-
☐	salvaguarda	Browse Structure Search Insert Empty Drop	5	InnoDB	latin1_swedish_ci	48 KiB	-
☐	salvaguarda_catalogo	Browse Structure Search Insert Empty Drop	17	InnoDB	latin1_swedish_ci	16 KiB	-
☐	valoracion	Browse Structure Search Insert Empty Drop	2	InnoDB	latin1_swedish_ci	48 KiB	-

Omar Brito y Abel Sierra.

La creación del menú principal aporta de manera importante en la construcción del esqueleto fundamental de la aplicación web. De acuerdo con lo establecido por MAGERIT en los libros de Catálogo de Elementos y en especial el de Guía de Técnicas, cada entidad tiene su función y propósito dentro del análisis y gestión de riesgos de sistemas de información. A continuación se define el propósito de cada entidad junto con sus atributos:

Proyecto – Sección donde se crea el proyecto base del análisis y gestión de riesgos informáticos. Sus atributos, también expuesto en la Figura 7, básicos consisten en ID del proyecto (valor que aumenta automáticamente), código (abreviatura del nombre del proyecto), propietario del proyecto, la organización a la que se implementará el análisis de riesgos informáticos, versión del proyecto, fecha y condición (propiedad intrínseca de la entidad dentro de la base de datos).

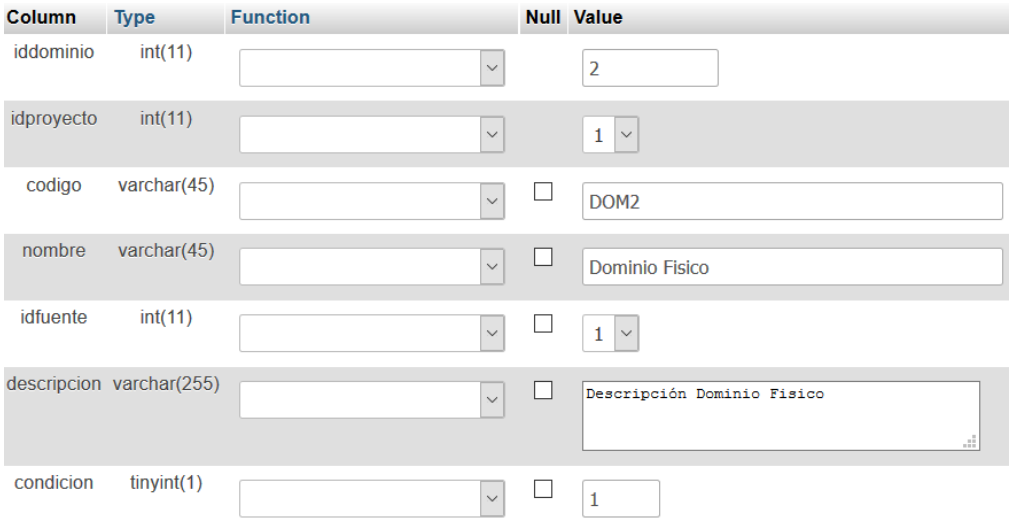
Figura 7. Atributos del proyecto



Omar Brito y Abel Sierra.

Dominio – Esta entidad tiene como atributos ID, código del dominio, nombre del dominio, descripción del dominio y, finalmente, el ID del proyecto, los cuales son ilustrados en la Figura 8. El ID del proyecto, como mencionado anteriormente, se escoge en Dominio para relacionarlo con el proyecto pertinente.

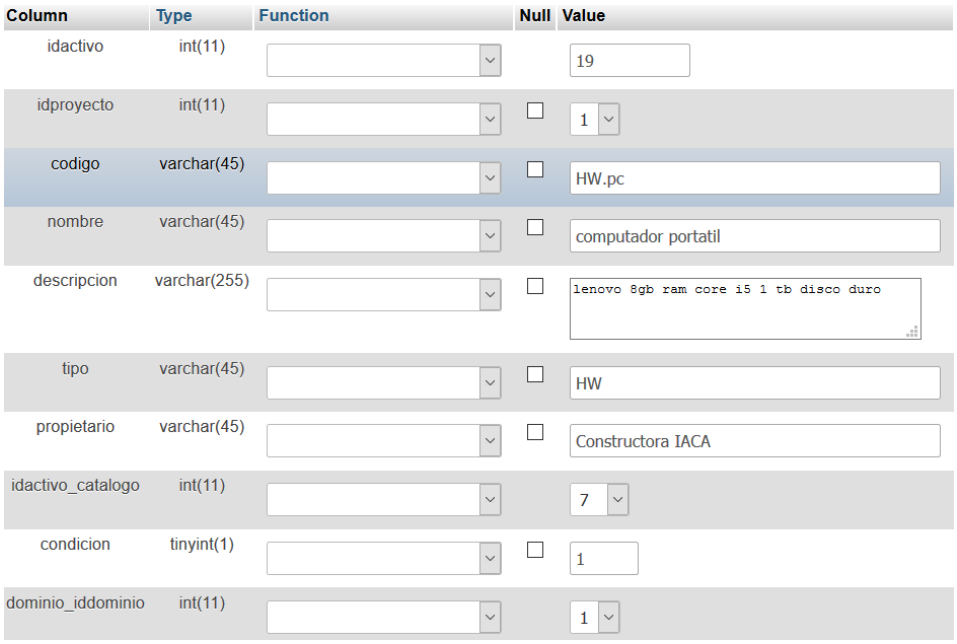
Figura 8. Atributos del dominio



Omar Brito y Abel Sierra.

Activo – Sección donde el usuario escoge el activo a ser analizado. Esta entidad es complementada por las entidades de datos predeterminados Activo_Catálogo y Descripción_Activo. El último se encarga de exponer los activos básicos pertenecientes a cada categoría. Los atributos, también listados en la Figura 9, que lo constituyen son ID de activo, ID de dominio, código de activo según MAGERIT, nombre del activo, descripción del activo, tipo de activo, propietario del activo, ID del catálogo y condición. La Figura 10 muestra la entidad Activo_Catálogo, que se encarga de exponer las categorías básicas con las cuales se clasifican los activos básicos del proyecto

Figura 9. Atributos del activo



Column	Type	Function	Null	Value
idactivo	int(11)			19
idproyecto	int(11)		☐	1
codigo	varchar(45)		☐	HW.pc
nombre	varchar(45)		☐	computador portatil
descripcion	varchar(255)		☐	lenovo 8gb ram core i5 1 tb disco duro
tipo	varchar(45)		☐	HW
propietario	varchar(45)		☐	Constructora IACA
idactivo_catalogo	int(11)			7
condicion	tinyint(1)		☐	1
dominio_iddominio	int(11)			1

Omar Brito y Abel Sierra.

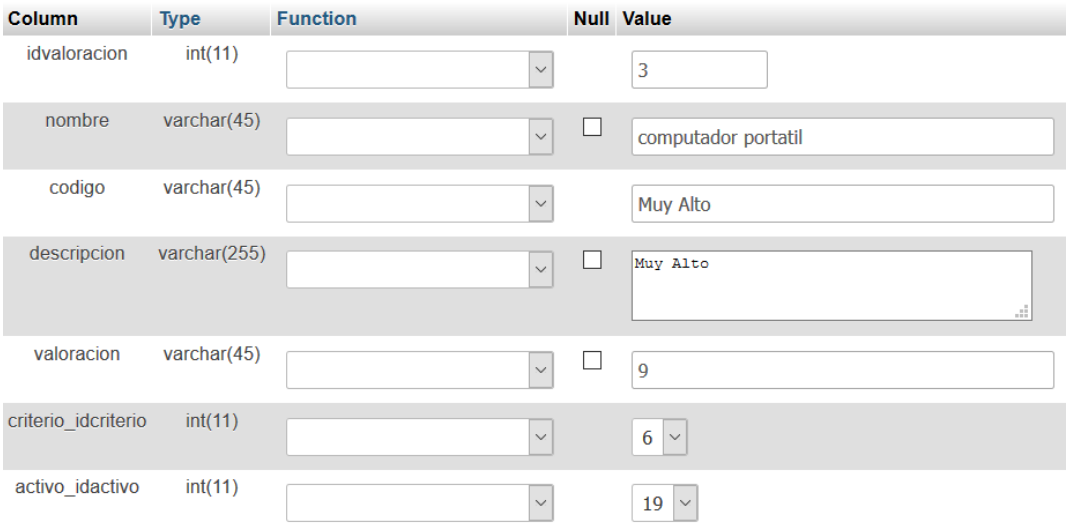
Figura 10. Catálogo de activos

	idactivo_catalogo	codigo	descripcion
☐ Edit Copy Delete	1	[essential]	Activos esenciales
☐ Edit Copy Delete	2	[arch]	Arquitectura del sistema
☐ Edit Copy Delete	3	[D]	Datos / Información
☐ Edit Copy Delete	4	[K]	Claves criptográficas
☐ Edit Copy Delete	5	[S]	Servicios
☐ Edit Copy Delete	6	[SW]	Software - Aplicaciones informáticas
☐ Edit Copy Delete	7	[HW]	Equipamiento informático (hardware)
☐ Edit Copy Delete	8	[COM]	Redes de comunicaciones
☐ Edit Copy Delete	9	[Media]	Soportes de información
☐ Edit Copy Delete	10	[AUX]	Equipamiento auxiliar
☐ Edit Copy Delete	11	[L]	Instalaciones
☐ Edit Copy Delete	12	[P]	Personal

Omar Brito y Abel Sierra.

Valoración – Sección donde se define el valor del activo según el criterio sugerido por MAGERIT. Sus atributos son ID de valoración, el nombre de la valoración, código, descripción de la valoración, el valor cualitativo de la valoración, el criterio por el cual se define la valoración, las cuales son ilustrados en la Figura 11. La Figura 12 muestra el catálogo de criterios, que es un esquema cualitativo en términos numéricos del 0 al 10

Figura 11. Atributos del valor



Column	Type	Function	Null	Value
idvaloracion	int(11)			3
nombre	varchar(45)		☐	computador portatil
codigo	varchar(45)			Muy Alto
descripcion	varchar(255)		☐	Muy Alto
valoracion	varchar(45)		☐	9
criterio_idcriterio	int(11)			6
activo_idactivo	int(11)			19

Omar Brito y Abel Sierra.

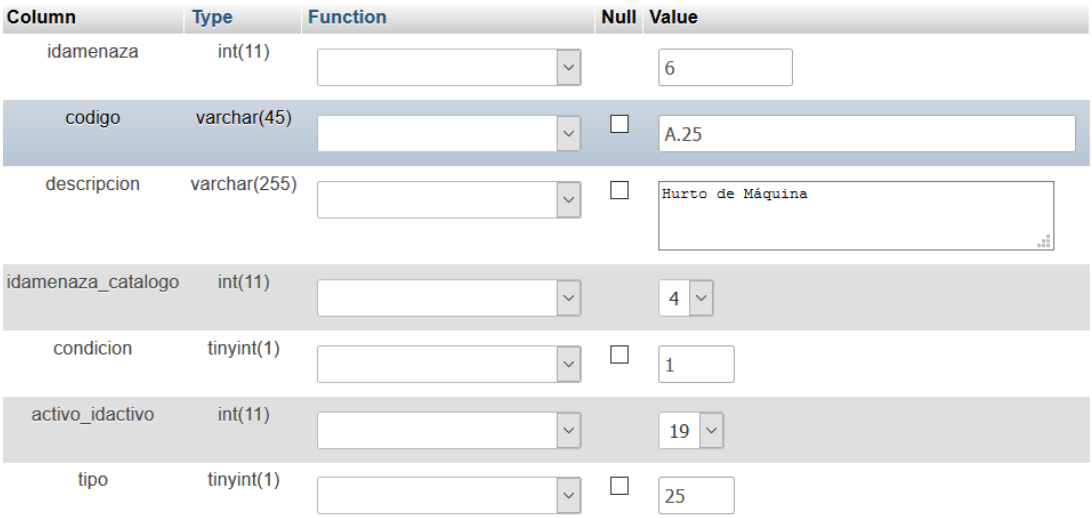
Figura 12. Catálogo de criterio

	idcriterio	codigo	descripcion	valori	valorf
☐ Edit Copy Delete	1	despreciable	irrelevante a efectos practicos	0	0
☐ Edit Copy Delete	2	bajo	daño menor	1	2
☐ Edit Copy Delete	3	medio	daño importante	3	5
☐ Edit Copy Delete	4	alto	daño grave	6	8
☐ Edit Copy Delete	5	muy alto	daño muy grave	9	9
☐ Edit Copy Delete	6	extremo	daño extremadamente grave	10	10

Omar Brito y Abel Sierra.

Amenaza – Sección donde el usuario escoge las amenazas asociadas al activo analizado. Esta entidad es a su vez complementada por las entidades de datos predeterminados Amenaza_Catálogo y Descripción_Amenaza. Sus atributos son ID de amenaza, código sugerido por MAGERIT, descripción de la amenaza, la categoría de la amenaza, condición y finalmente el ID del activo, todos también ilustrados en la Figura 13. Amenaza_Catálogo, ilustrada en la Figura 14, lista las categorías básicas por las cuales se clasifican las amenazas listadas en Descripción_Amenaza.

Figura 13. Atributos de amenaza



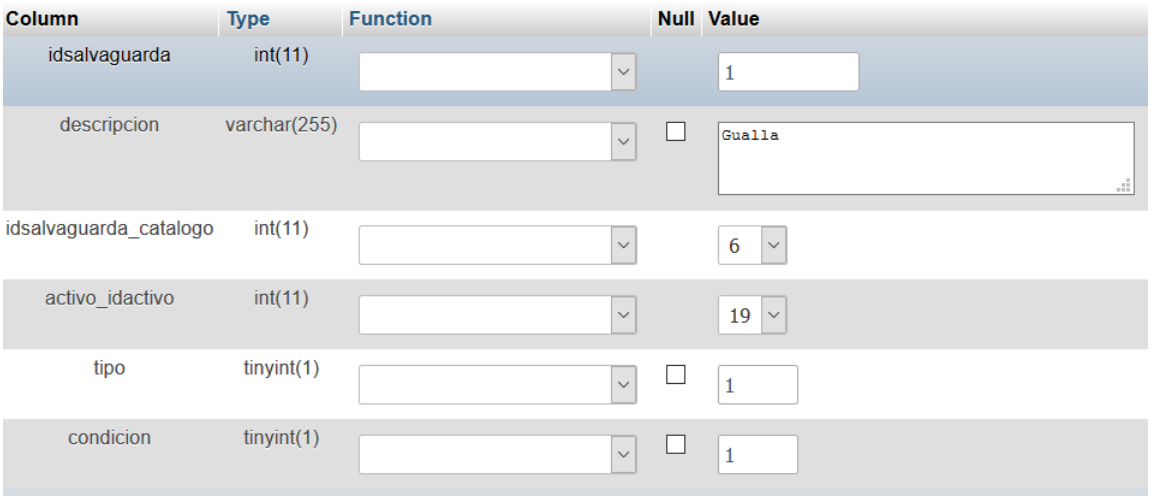
Omar Brito y Abel Sierra.

Figura 14. Catálogo de amenaza

Omar Brito y Abel Sierra.

Salvaguarda – Sección donde el usuario escoge desde un catálogo una salvaguarda sugerida por MAGERIT. Sus atributos, ilustrados también en la Figura 15, son ID de salvaguarda, descripción de la salvaguarda e ID del catálogo de salvaguardas a la que corresponde aquella escogida.

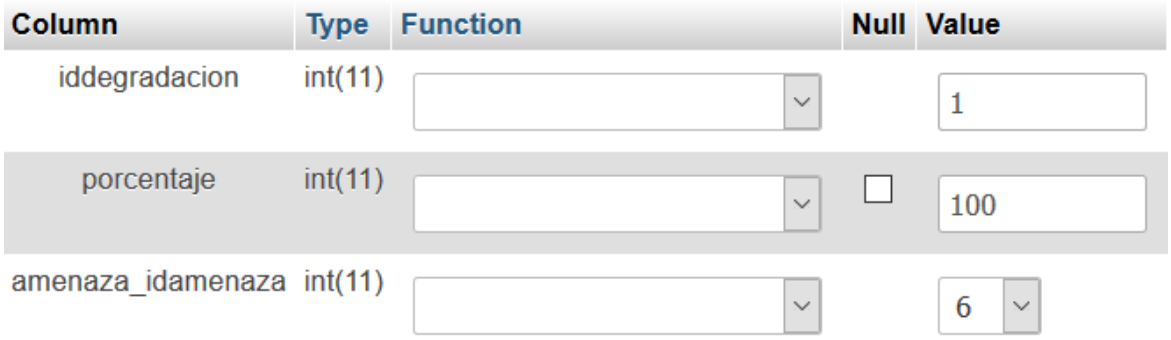
Figura 15. Atributos de salvaguarda



Omar Brito y Abel Sierra.

Degradación – Sección donde el usuario ingresa el valor de la degradación pertinente a la amenaza que afectará al activo. Los atributos que la constituyen son ID de degradación, el valor de la degradación (según MAGERIT es un valor decimal entre 0,0 y 1,0 o un porcentaje) y el ID de la amenaza, todos incluidos en la Figura 16.

Figura 16. Atributos de degradación

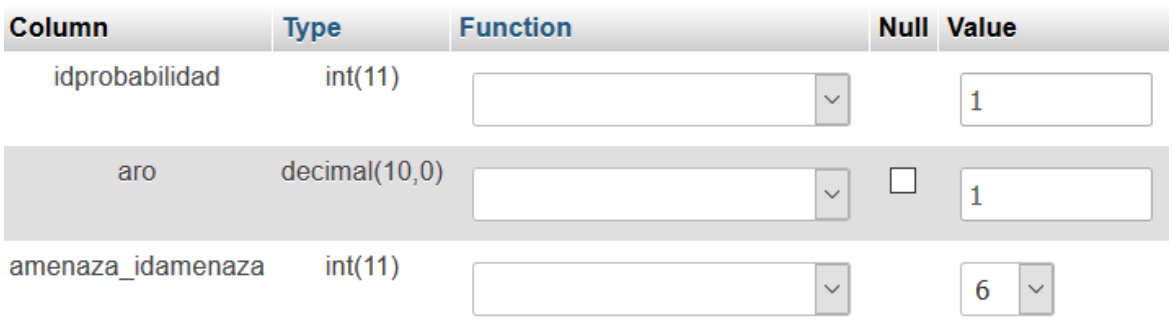


Column	Type	Function	Null	Value
iddegradacion	int(11)			1
porcentaje	int(11)		☐	100
amenaza_idamenaza	int(11)			6

Omar Brito y Abel Sierra.

Probabilidad – Sección donde el usuario ingresa el valor del número de ocurrencias de una amenaza por año sobre el activo. La presente entidad, representada en la Figura 17, es constituida por el ID de la probabilidad, ARO o la probabilidad de ocurrencia de la amenaza en un año y el ID de la amenaza.

Figura 17. Atributos de probabilidad

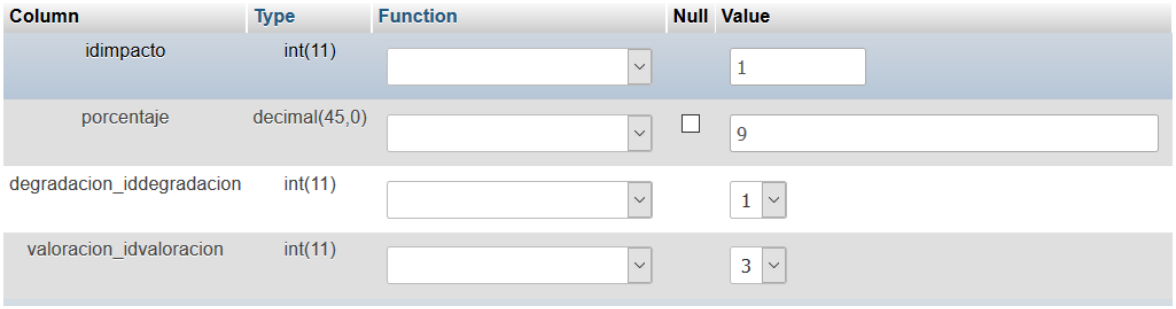


Column	Type	Function	Null	Value
idprobabilidad	int(11)			1
aro	decimal(10,0)		☐	1
amenaza_idamenaza	int(11)			6

Omar Brito y Abel Sierra.

Impacto – Sección donde se revela el resultado de la degradación por el valor del activo. Sus atributos son el ID del impacto, ID de la degradación, ID de la valoración del activo y porcentaje, los cuales son también ilustrados en Figura 18.

Figura 18. Atributos de impacto

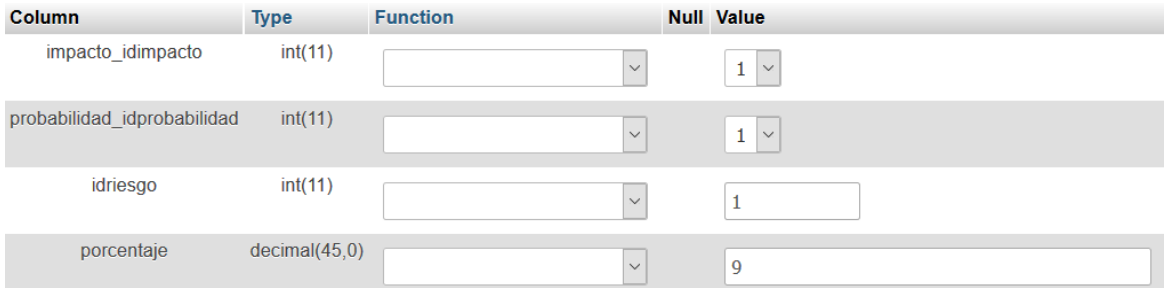


Column	Type	Function	Null	Value
idimpacto	int(11)			1
porcentaje	decimal(45,0)			9
degradacion_iddegradacion	int(11)			1
valoracion_idvaloracion	int(11)			3

Omar Brito y Abel Sierra.

Riesgo – La Figura 19 muestra una sección donde se expone el resultado de la probabilidad de ocurrencia por el impacto. Similar a como es constituido el impacto, el riesgo tiene los siguientes atributos: ID del riesgo, ID del impacto, ID de la probabilidad de ocurrencia de la amenaza y porcentaje.

Figura 19. Atributos de riesgo

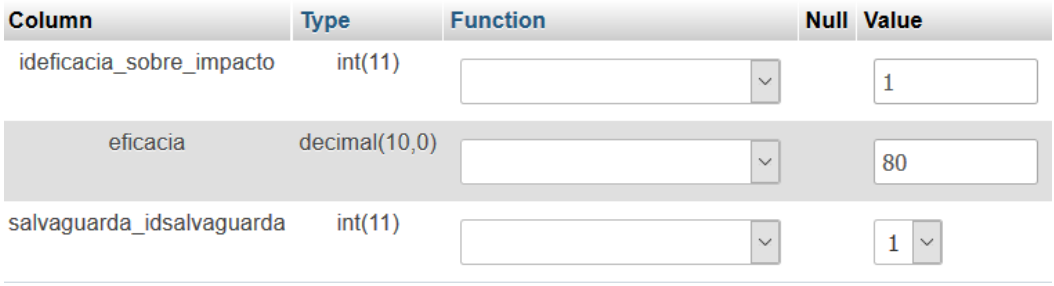


Column	Type	Function	Null	Value
impacto_idimpacto	int(11)			1
probabilidad_idprobabilidad	int(11)			1
idriesgo	int(11)			1
porcentaje	decimal(45,0)			9

Omar Brito y Abel Sierra.

Eficacia sobre Impacto – Sección donde el usuario ingresa en términos numéricos el efecto que genera una salvaguarda sobre el impacto que una amenaza le ocasiona a un activo. Sus atributos, ilustrados también en la Figura 20, son ID de eficacia sobre impacto, el valor de la eficacia sobre impacto (según MAGERIT es un número decimal entre 0,0 y 1,0 o porcentaje), ID de la amenaza y finalmente el ID de la salvaguarda.

Figura 20. Eficacia sobre impacto

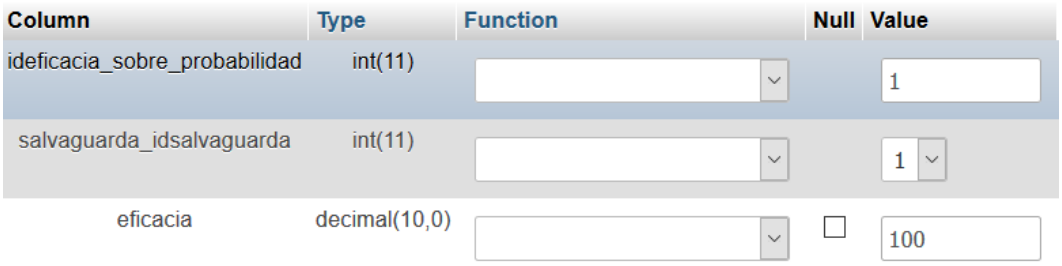


Column	Type	Function	Null	Value
ideficacia_sobre_impacto	int(11)			1
eficacia	decimal(10,0)			80
salvaguarda_idsalvaguarda	int(11)			1

Omar Brito y Abel Sierra.

Eficacia sobre Probabilidad – Sección donde el usuario ingresa en términos numéricos el efecto que le proporciona una salvaguarda a la probabilidad de ocurrencia de una amenaza sobre el activo. Sus atributos son ID de eficacia sobre la probabilidad, el valor de la eficacia sobre la probabilidad (según MAGERIT es un número decimal entre 0,0 y 1,0 o porcentaje), ID de la amenaza y finalmente el ID de la salvaguarda, todos también ilustrados en la Figura 21.

Figura 21. Eficacia sobre probabilidad

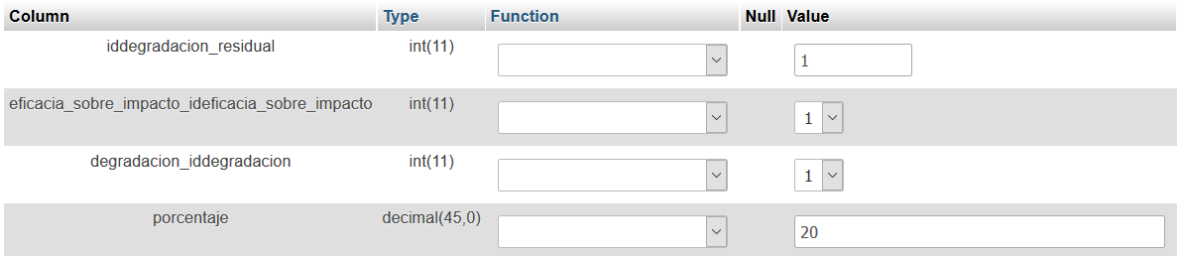


Column	Type	Function	Null	Value
ideficacia_sobre_probabilidad	int(11)			1
salvaguarda_idsalvaguarda	int(11)			1
eficacia	decimal(10,0)		☐	100

Omar Brito y Abel Sierra.

Degradación Residual – Sección donde se calcula y expone el resultado de la salvaguarda contra la degradación ocasionada por una amenaza en particular. Sus atributos, ilustrados también en la Figura 22, son el ID de la degradación residual, el ID de la eficacia sobre el impacto, el ID de la degradación y porcentaje.

Figura 22. Atributos de degradación residual

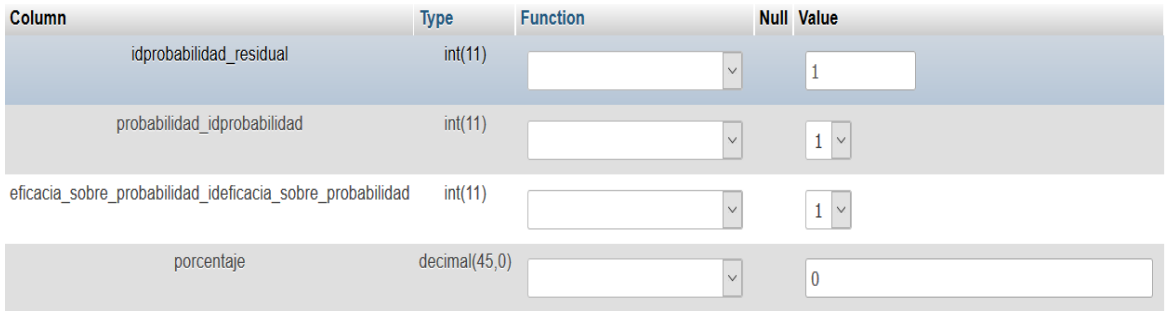


Column	Type	Function	Null	Value
iddegradacion_residual	int(11)			1
eficacia_sobre_impacto_ideficacia_sobre_impacto	int(11)			1
degradacion_iddegradacion	int(11)			1
porcentaje	decimal(45,0)			20

Omar Brito y Abel Sierra.

Probabilidad Residual – Sección donde se calcula y revela el resultado de la salvaguarda contra la probabilidad de ocurrencia de una amenaza sobre el activo. Similar a como es construido la degradación residual y tomando como base la Figura 23, la probabilidad residual se construye a partir de los atributos ID de probabilidad residual, el ID de la eficacia sobre la probabilidad e ID de la probabilidad de ocurrencia originalmente digitada por el usuario.

Figura 23. Atributos de probabilidad residual

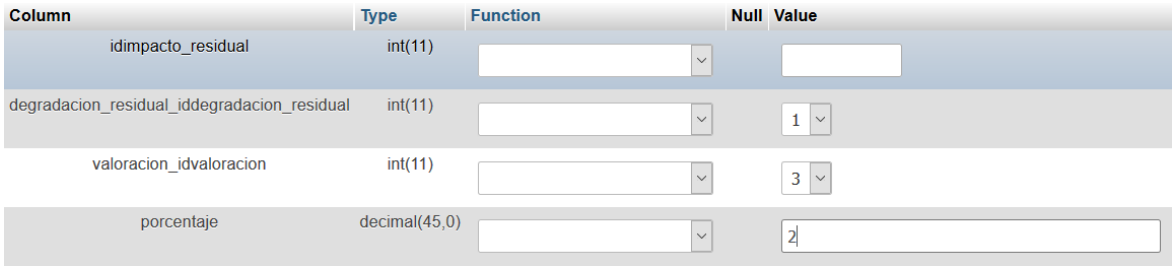


Column	Type	Function	Null	Value
idprobabilidad_residual	int(11)			1
probabilidad_idprobabilidad	int(11)			1
eficacia_sobre_probabilidad_ideficacia_sobre_probabilidad	int(11)			1
porcentaje	decimal(45,0)			0

Omar Brito y Abel Sierra.

Impacto Residual – Sección donde se calcula y expone el valor de la degradación residual por el valor del activo. Sus atributos son el ID del impacto residual, ID de la degradación residual y el ID de la valoración del activo originalmente escogida por el usuario, todos ilustrados también en la Figura 24.

Figura 24. Atributos de impacto residual

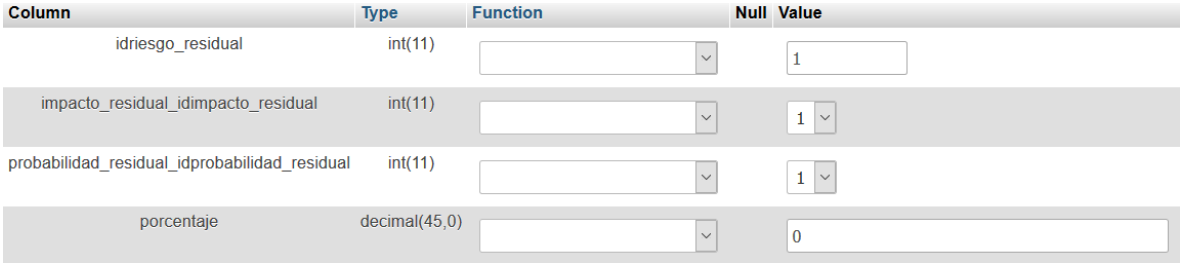


Column	Type	Function	Null	Value
idimpacto_residual	int(11)			
degradacion_residual_iddegradacion_residual	int(11)			1
valoracion_idvaloracion	int(11)			3
porcentaje	decimal(45,0)			2

Omar Brito y Abel Sierra.

Riesgo Residual – Sección donde se calcula y expone el valor de la probabilidad residual por el impacto residual. Por último, como mostrado en la Figura 25, sus componentes son el ID del riesgo residual, el ID del impacto residual y el ID de la probabilidad residual.

Figura 25. Atributos de riesgo residual



Column	Type	Function	Null	Value
idriesgo_residual	int(11)			1
impacto_residual_idimpacto_residual	int(11)			1
probabilidad_residual_idprobabilidad_residual	int(11)			1
porcentaje	decimal(45,0)			0

Omar Brito y Abel Sierra.

Previo al desarrollo de la base de datos, se encontró que el usuario tiene tres formas de interacción con la aplicación. Todas tres son definidas por el rol que tiene cada elemento descrito en Libro III – Guía de Técnicas. A continuación, se listan las tres formas de interacción que la aplicación web deberá tener con el usuario final:

- Ingreso de Datos por Tabla – En esta categoría hacen parte el activo, la valoración del activo, la amenaza y la salvaguarda. El usuario deberá escoger la información para estas entidades a partir de las tablas expuestas en Libro II - Catálogo de Elementos.

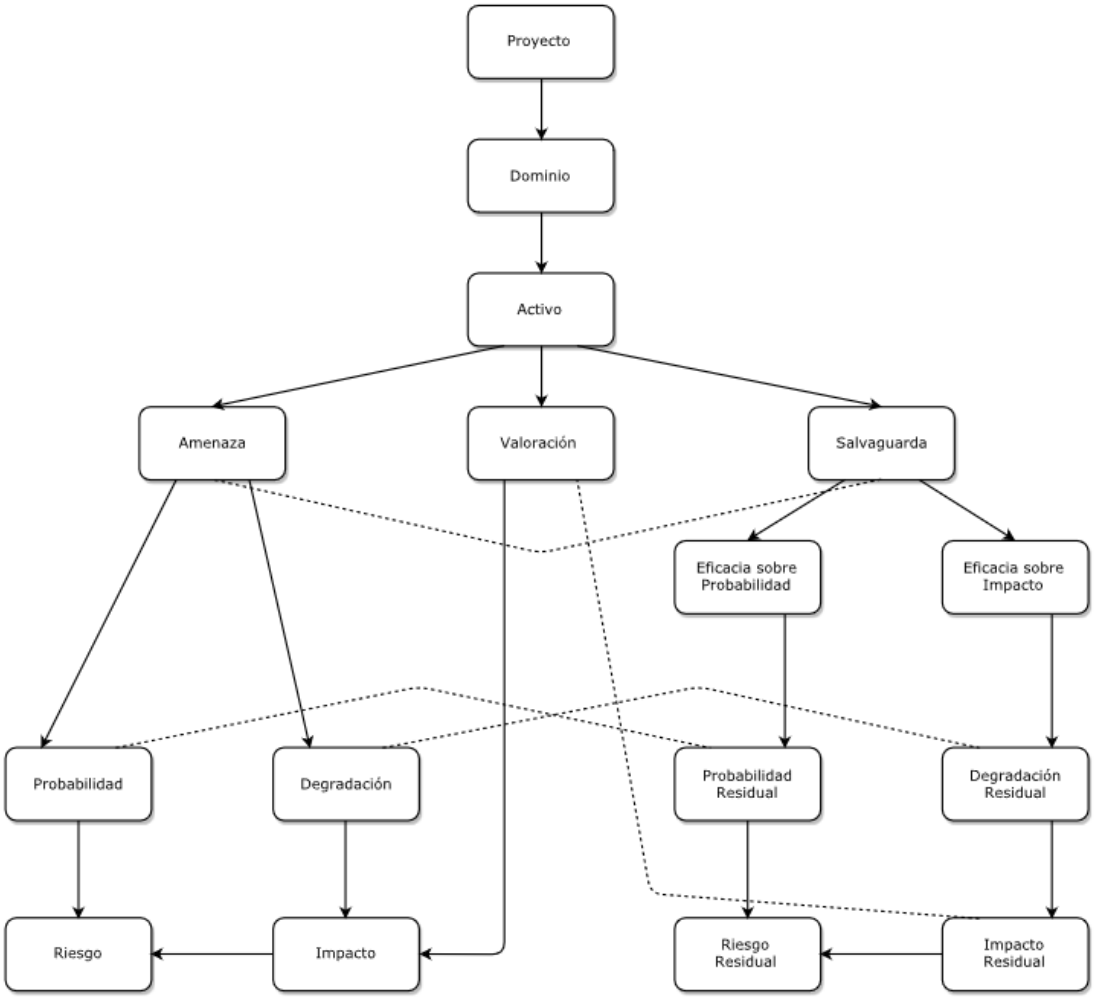
- Ingreso de Valores por Usuario – En esta categoría entran la degradación, la probabilidad de ocurrencia, la eficacia sobre el impacto y la eficacia sobre la probabilidad, en las cuales el usuario deberá ingresar valores numéricos.

- Cálculo de Valores por Aplicación – En esta categoría entran el impacto, el riesgo, la degradación residual, la probabilidad residual, el impacto residual y el riesgo residual, de las cuales que el usuario recibirá el cálculo automático de sus resultados.

Las relaciones entre las entidades, las unidades de sus valores y el proceso básico por el cual se calculan resultados fueron construidas tomando como base bibliográfica Libro III – Guía de Técnicas de MAGERIT. No obstante, para el desarrollo eficaz de la aplicación, hubo consideraciones configurativas importantes propias del proyecto, entre los cuales el más notorio es el llamado al ID del activo en la mayoría de las entidades presentadas, la cual permitió la correlación entre los activos y el resto de las entidades. Por ende, la base de datos, la aplicación y los resultados están centrados en torno a los activos seleccionados.

Dado que Libro III – Guía de Técnicas presenta las relaciones entre entidades (las cuales son mencionadas en el marco teórico del presente trabajo escrito), se concluye que también presenta una secuencia en el que se deben diligenciar los datos y calcular los resultados. Dicha secuencia también fue tomada en cuenta durante el desarrollo de la aplicación web. El factor determinador de dicha secuencia es el uso de los IDs, cuyo rol consiste en asignar un número identificador por grupo de atributos ingresados en la entidad. Luego, cuando el usuario procede a llenar los atributos de subsiguientes entidades, éstas solicitarán el ID de aquellas entidades de las cuales dependen. Si existe alguna que no fue debidamente diligenciada por el usuario, las siguientes entidades que dependen de aquella en mención no podrán ser diligenciadas ni calculadas. La secuencia se ilustra en el diagrama de flujo de la Figura 26, cuyo orden comienza desde Proyecto hacia abajo. Las flechas señalan la secuencia y las dependencias entre las entidades (las flechas continuas y discretas no tienen diferencia de significado).

Figura 26. Diagrama de flujo de base de datos



Omar Brito y Abel Sierra.

5.5 IMPLEMENTACIÓN DE LA APLICACIÓN WEB

De acuerdo con el orden, la semántica y la implementación de la base de datos, se procede con la implementación de la aplicación en Laravel basado en el lenguaje PHP, cuyo esquema básicamente asume las entidades definidas anteriormente junto con sus atributos. En esta etapa la interacción entre la aplicación web y la base de datos es importante ya que los valores ingresados en la aplicación deben ser almacenados en la base de datos. Por ende, como mencionado anteriormente, los atributos usados en la base de datos deben ser mapeados para su uso en la

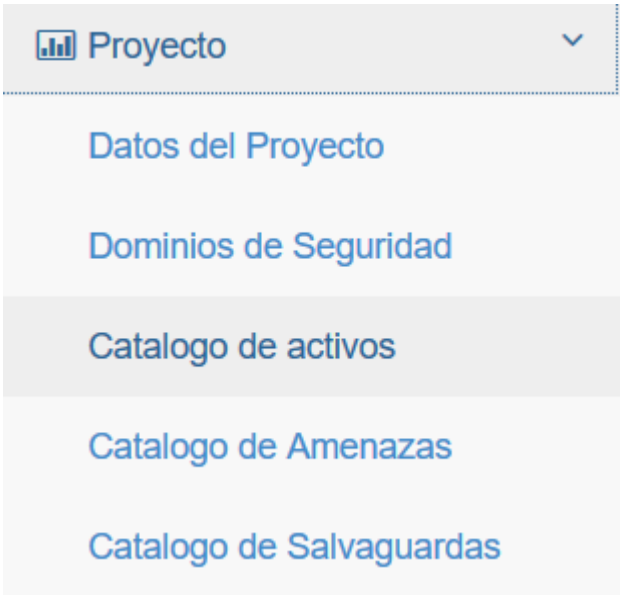
aplicación web, tanto en el *backend* como en el *frontend*. Dicho mapeo permite entender la función de las entidades y sus atributos, tal que permite la agrupación de entidades en tres grandes grupos, que a su vez fueron usados para el diseño del menú principal: Proyecto, Análisis de Riesgos e Informes.

La estructura visual de la aplicación fue diseñada para ayudar al usuario en su uso, con las entidades listadas a la izquierda de la ventana separadas en los tres grupos anteriormente mencionados, una descripción de terminología y comentarios en la parte superior de cada entidad seleccionada, una lista de elementos y resultados en la parte central de cada entidad seleccionada, y los botones de creación, edición y eliminación de datos al final de cada entidad seleccionada.

Al ingresar a la aplicación, el usuario notará que cada entidad cuenta con herramientas cuyos propósitos son facilitar su interacción con la aplicación. Además de los botones anteriormente mencionados, existen entidades que cuentan con espacios para la búsqueda interactiva de información basados en el ingreso de palabras o letras, paginación para la visualización de todos los datos de un catálogo, barras deslizadoras para la selección de valores porcentuales y espacios dentro de los cuales el usuario podrá ingresar valores exactos. A continuación, se revela la implementación final de la aplicación web de libre uso, junto con imágenes que contienen información de la interfaz gráfica y de los valores reales que se usaron para realizar pruebas. La aplicación web es capaz de recibir nueva información seleccionada por el usuario de acuerdo con los catálogos y valores digitados, es capaz de editar datos previamente ingresados, eliminar datos previamente ingresados y calcular resultados tanto a nivel de impacto, riesgo, y los valores residuales. Finalmente, cabe mencionar, que la información acerca del código fuente de la totalidad del proyecto, tanto base de datos como aplicación web, se encuentra provista, la cual para apreciar su funcionamiento es necesario su instalación localmente en un computador.

Proyecto – Como ilustrado en la Figura 27, esta entidad consta de sectores donde el usuario debe diligenciar los datos básicos de la creación del proyecto, crear los dominios de seguridad y donde el usuario halla referencias de los elementos relacionados con los criterios de valoración, activos, amenazas y salvaguardas que se encuentran en el Libro II – Catálogo de Elementos.

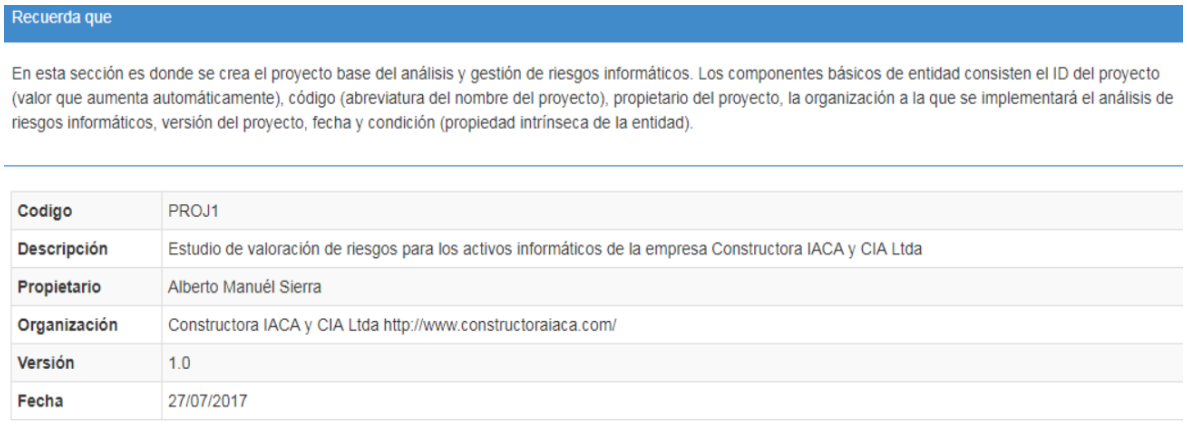
Figura 27. Categoría proyecto



Omar Brito y Abel Sierra.

Datos del Proyecto se refiere a la entidad Proyecto de la base de datos, donde el usuario diligencia los datos básicos de la creación del proyecto para el análisis y la gestión de riesgos de los sistemas de la información. Figura 28 presenta un ejemplo de un proyecto creado, cuya información fue provista por Constructora IACA y CIA Ltda.

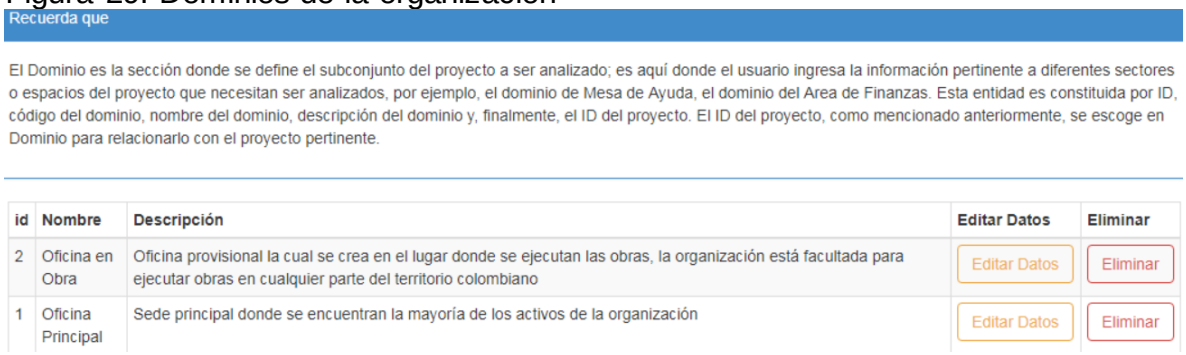
Figura 28. Datos del proyecto



Omar Brito y Abel Sierra.

Figura 29 muestra la entidad Dominios de Seguridad, donde el usuario tiene la posibilidad de subdividir el proyecto en grupos de activos para proporcionar un enfoque en el análisis.

Figura 29. Dominios de la organización



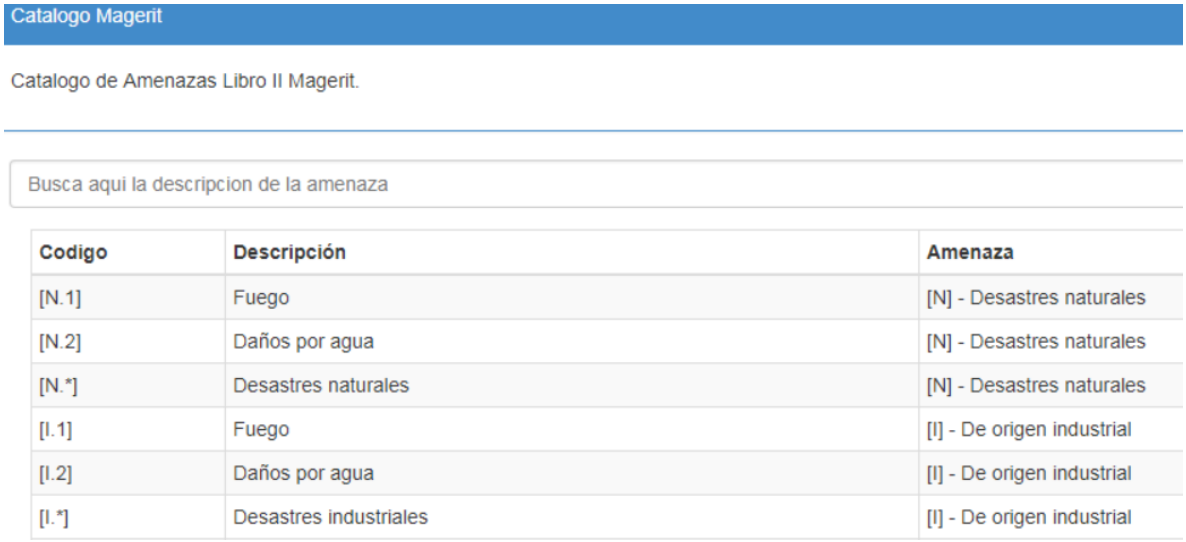
Omar Brito y Abel Sierra.

Basado en las entidades de catálogo de elementos en la base de datos, específicamente Descripción_Activo, Descripción_Amenaza y Descripción_Salvaguarda, la aplicación también tiene listas de elementos para que funcionen como referencia para la selección de activos, amenazas y salvaguardas. Dado que existe un gran número de elementos, cada sector cuenta con un espacio para realizar la búsqueda de un elemento en específico. Lo anterior se visualiza en la Figura 30 para Catálogo de Activos y la Figura 31 para Catálogo de Amenazas.

Figura 30. Catálogo de activos

Omar Brito y Abel Sierra.

Figura 31. Catálogo de amenazas



Omar Brito y Abel Sierra.

Finalmente, de acuerdo a lo anterior, la Figura 32 muestra los elementos listados bajo Catálogo de Amenazas.

Figura 32. Catálogo de salvaguardas

Codigo	Descripción	Salvaguarda
H	Protecciones Generales	Protecciones generales u horizontales
H.IA	Identificación y autenticación	Protecciones generales u horizontales
H.AC	Control de acceso lógico	Protecciones generales u horizontales
H.ST	Segregación de tareas	Protecciones generales u horizontales
H.IR	Gestión de incidencias	Protecciones generales u horizontales
H.tools	Herramientas de seguridad	Protecciones generales u horizontales
H.tools.AV	Herramienta contra código dañino	Protecciones generales u horizontales

Omar Brito y Abel Sierra.

Análisis de Riesgos – La Figura 33 muestra el sector de Análisis de Riesgos, el cual está diseñado para la recepción de datos y para la generación de resultados, donde la primera consta de entidades de diligenciamiento de información como la escogencia de activos, amenazas, salvaguardas, valoración, y mientras que la última consiste en el ingreso de datos de degradación, probabilidad, eficacia sobre impacto y eficacia sobre probabilidad. Para ello permanecen las mismas relaciones directas que fueron establecidas durante el desarrollo de la base de datos. Adicionalmente, cada entidad de este sector cuenta con información general de la terminología usada, ubicada normalmente en la parte superior de la vista.

Figura 33. Análisis de riesgos

Omar Brito y Abel Sierra.

Similar a lo expuesto en la base de datos, la entidad Activos hace uso de la entidad Catálogo de Activos. De igual manera, Amenazas y Salvaguardas hacen uso de Catálogo de Amenazas y Catálogo de Salvaguardas, respectivamente. Adicionalmente, los atributos son similares en las tres entidades y considerando la facultad de búsqueda de elementos en los espacios donde se diligencian datos, la aplicación le proporciona al usuario facilidad de interacción con el programa. Teniendo en cuenta la descripción anterior, Figura 34 y Figura 35 ilustran las entidades Activos y Amenazas, respectivamente.

Figura 34. Activos

id	Nombre	Descripción	Catalogo	Descripción Magerit	Dominio	Editar	Eliminar
12	Archivador	archivador metálico de 3 puestos	[Media] - Soportes de información	[printed] - material impreso	Oficina Principal	Editar	Eliminar
11	Disco Duro portátil	Western Digital 1 tb	[Media] - Soportes de información	[disk] - discos	Oficina Principal	Editar	Eliminar
10	Memoria USB	Memorias usb 4 y 8 gb para el uso diario	[Media] - Soportes de información	[usb] - memorias USB	Oficina Principal	Editar	Eliminar
9	Router (Conexión a Internet)	Router arris tg862	[COM] - Redes de comunicaciones	[Internet] - Internet	Oficina Principal	Editar	Eliminar

Omar Brito y Abel Sierra.

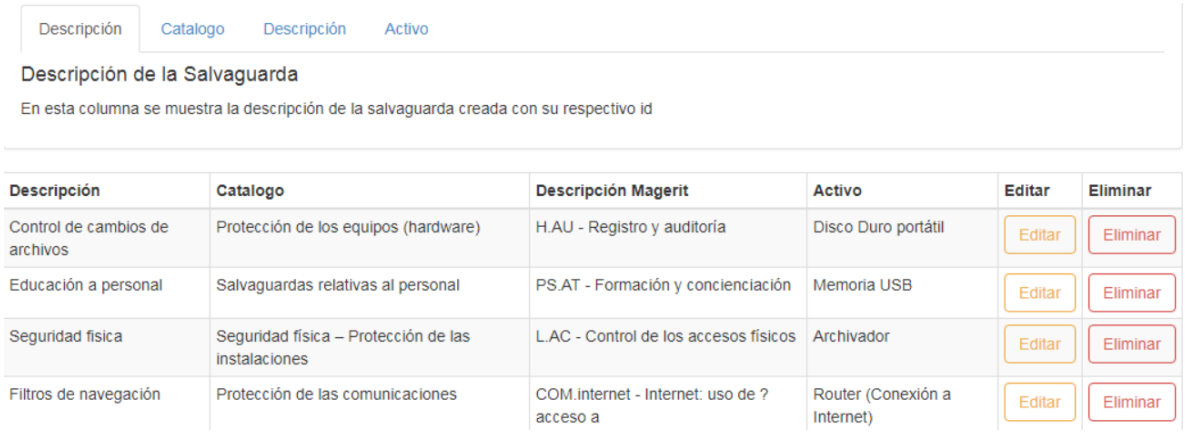
Figura 35. Amenazas

id	Nombre	Catalogo	Descripcion	Activo	Editar	Eliminar
12	Cambios en los archivos	[A] - Ataques intencionados	[A.15] - Modificación deliberada de la información	Disco Duro portátil	Editar Datos	Eliminar
11	perdida	[E] - Errores y fallos no intencionados	[E.25] - Pérdida de equipos	Memoria USB	Editar Datos	Eliminar
10	Acceso a archivos fisicos	[A] - Ataques intencionados	[A.6] - Abuso de privilegios de acceso	Archivador	Editar Datos	Eliminar
9	Saturación de ancho de banda	[E] - Errores y fallos no intencionados	[E.24] - Caída del sistema por agotamiento de recursos	Router (Conexión a Internet)	Editar Datos	Eliminar

Omar Brito y Abel Sierra.

Finalmente, la Figura 36 ilustra la entidad Salvaguardas.

Figura 36. Salvaguardas



Omar Brito y Abel Sierra.

La entidad Valoración proporciona un espacio para ingresar el valor cualitativo del activo previamente escogido. Dichos valores cualitativos se basan en aquellos propuestos por MAGERIT en el Libro II – Catálogo de Elementos. Tal como en los sectores pasados, los campos brindan ayuda al listar las opciones pertinentes, los cuales son filtrados cuando el usuario ingresa una palabra o letras. La Figura 37 demuestra su función dentro de la aplicación web.

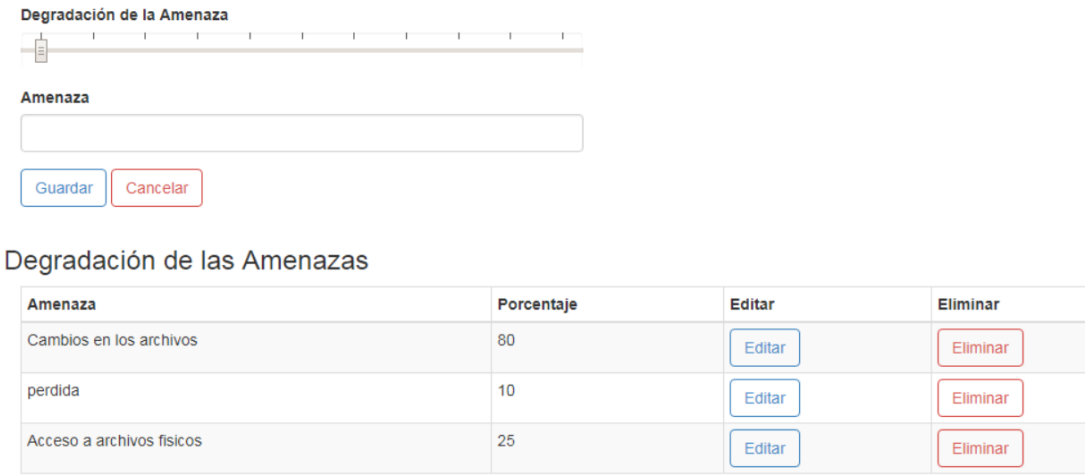
Figura 37. Valoración de activos

Omar Brito y Abel Sierra.

Las entidades Degradación, Probabilidad, Eficacia/Impacto y Eficacia/Probabilidad son espacios donde el usuario debe ingresar datos, sean estos datos porcentuales

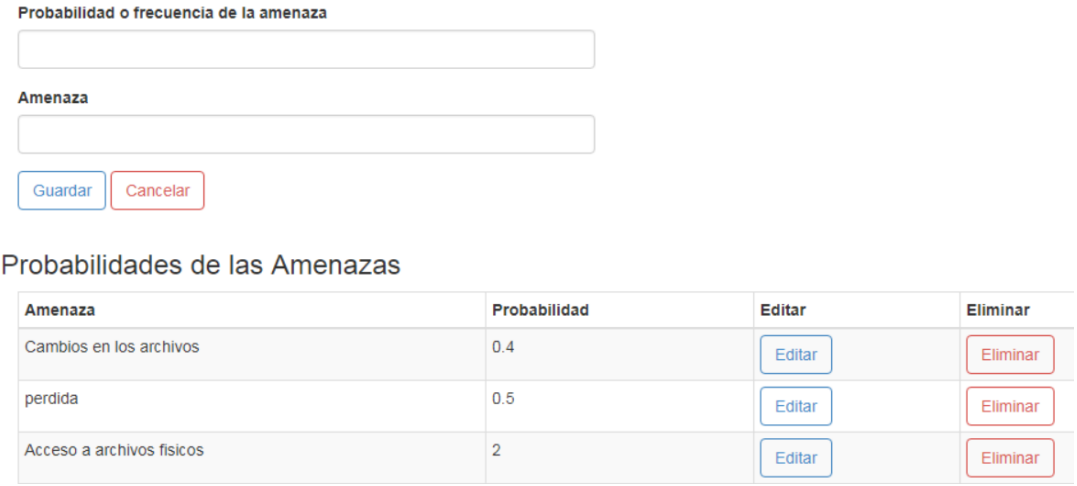
(como es el caso de Degradación, Eficacia/Impacto y Eficacia/Probabilidad) como datos numéricos flotantes (como es el caso de Probabilidad). Como se visualiza Degradación en la Figura 38, Probabilidad de Ocurrencia en la Figura 39, Eficacia sobre Impacto en la Figura 40 y a su vez Eficacia sobre Probabilidad de Ocurrencia en la Figura 41, aquellas entidades que reciben datos porcentuales ofrecen el uso de una barra en el que el usuario tiene a su disposición graduar para escoger el porcentaje adecuado.

Figura 38. Degradación



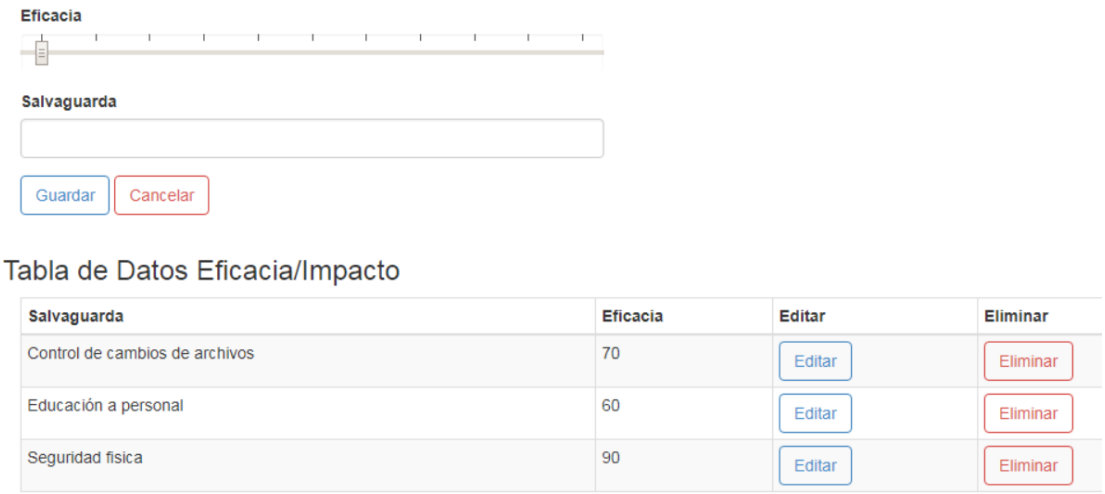
Omar Brito y Abel Sierra.

Figura 39. Probabilidad de ocurrencia



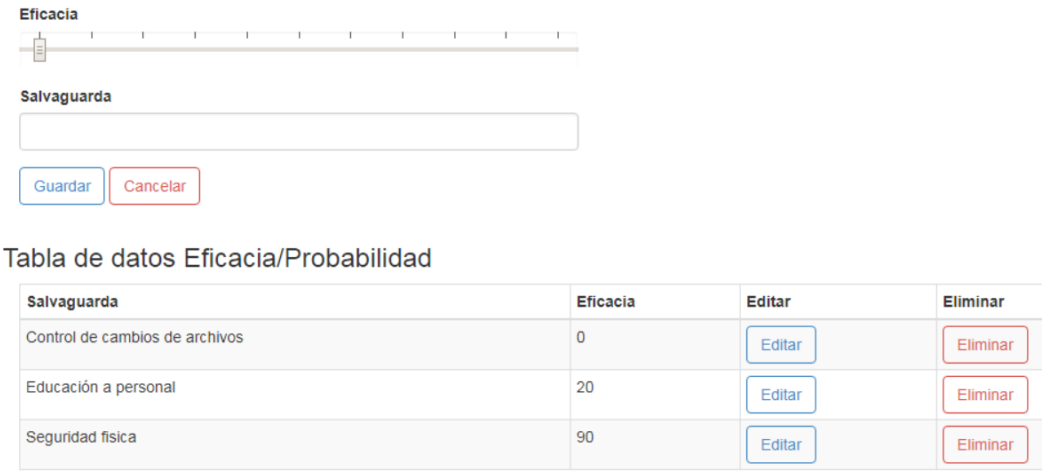
Omar Brito y Abel Sierra.

Figura 40. Eficacia sobre impacto



Omar Brito y Abel Sierra.

Figura 41. Eficacia sobre probabilidad de ocurrencia



Omar Brito y Abel Sierra.

Finalmente, dentro del sector Análisis de Riesgo, la aplicación proporciona las entidades que ofrecen el cálculo automático de los valores ingresados en las entidades anteriores. El cálculo automático de resultados toma como datos aquellos ingresados en las entidades anteriores, y sus respuestas son automáticamente almacenadas en la base de datos. El usuario final tendrá la facilidad de ver dichos resultados al invocarlos en la aplicación web las veces que se desee. Estas hacen referencia a Impacto, Riesgo, Degradación Residual, Probabilidad de Ocurrencia Residual e Impacto Residual, ilustradas en las siguientes páginas en Figura 42,

Figura 43, Figura 44, Figura 45 y Figura 46, respectivamente. Cada una de ellas cuenta con un botón para activar el cálculo automáticamente.

Figura 42. Impacto

El Impacto es la reducción de valor de activo como consecuencia que sobre un activo tiene la materialización de una amenaza. El impacto usualmente se mide con las mismas unidades del valor del activo y es el producto final entre dicho valor y la degradación.

Activo	Amenaza	Valor
Disco Duro portátil	Cambios en los archivos	5.6
Memoria USB	perdida	0.3
Archivador	Acceso a archivos fisicos	2
Router (Conexión a Internet)	Saturación de ancho de banda	6.4
Impresora Multifuncional	Daño de equipo	1.5
Computador Portátil	Hurto de Maquina	9

Omar Brito y Abel Sierra.

Figura 43. Riesgo

El Riesgo es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización . Sus unidades se definen en el valor del activo sobre un año y resulta siendo el producto entre la probabilidad de ocurrencia de la amenaza y el impacto que este ocasiona sobre el activo.

Activo	Amenaza	Valor
Disco Duro portátil	Cambios en los archivos	2.24
Memoria USB	perdida	0.15
Archivador	Acceso a archivos fisicos	4
Router (Conexión a Internet)	Saturación de ancho de banda	128
Impresora Multifuncional	Daño de equipo	6
Computador Portátil	Hurto de Maquina	0.9

Omar Brito y Abel Sierra.

Figura 44. Degradación residual

Degradación Residual – La degradación remanente luego que una amenaza se materialice sobre un activo que posee alguna salvaguarda. Técnicamente, es el producto entre la degradación y la efectividad de la salvaguarda sobre el impacto. Degradación_Residual=Degradación × Efectividad_Impacto

Amenaza	Salvaguarda	Valor
Cambios en los archivos	Control de cambios de archivos	0.24
perdida	Educación a personal	0.04
Acceso a archivos fisicos	Seguridad fisica	0.025
Saturación de ancho de banda	Filtros de navegación	0.56
Daño de equipo	Ventilación	0.03
Hurto de Maquina	Gualla	0.2

Omar Brito y Abel Sierra.

Figura 45. Probabilidad de ocurrencia residual

La Probabilidad Residual es la probabilidad de ocurrencia remanente luego que una amenaza se materialice sobre un activo que posee alguna salvaguarda. La probabilidad residual es el producto entre la probabilidad de ocurrencia y la efectividad de la salvaguarda sobre la probabilidad. Probabilidad_Residual=Probabilidad ×Efectividad_Probabilidad

Amenaza	Salvaguarda	Valor
Cambios en los archivos	Control de cambios de archivos	0.4
perdida	Educación a personal	0.4
Acceso a archivos fisicos	Seguridad fisica	0.2
Saturación de ancho de banda	Filtros de navegación	14
Daño de equipo	Ventilación	2
Hurto de Maquina	Gualla	0

Omar Brito y Abel Sierra.

Figura 46. Impacto residual

El Impacto Residual es el impacto final luego de la materialización de una amenaza sobre un activo que a su vez tiene una salvaguarda que reduce la degradación que potencialmente produciría dicha amenaza sobre un activo. Su resultado se halla como el producto del valor del activo y de la degradación residual. Impacto_Residual=Valor × Degradación_Residual

Activo	Amenaza	Valor
Disco Duro portátil	Cambios en los archivos	1.68
Memoria USB	perdida	0.12
Archivador	Acceso a archivos fisicos	0.2
Router (Conexión a Internet)	Saturación de ancho de banda	4.48
Impresora Multifuncional	Daño de equipo	0.15
Computador Portátil	Hurto de Maquina	1.8

Omar Brito y Abel Sierra.

Finalmente, el Riesgo Residual en la Figura 47 es la última entidad con las mismas características que aquellas ilustradas anteriormente.

Figura 47. Riesgo residual

El Riesgo Residual es el riesgo final luego de la materialización de una amenaza sobre un activo que a su vez tiene una salvaguarda que reduce su probabilidad de ocurrencia. El riesgo residual se halla como el producto del Impacto Residual y de la Probabilidad Residual. Riesgo_Residual=Impacto_Residual× Probabilidad_Residual

Activo	Amenaza	Salvaguarda	Valor
Disco Duro portátil	Cambios en los archivos	Control de cambios de archivos	0.672
Memoria USB	perdida	Educación a personal	0.048
Archivador	Acceso a archivos fisicos	Seguridad fisica	0.04
Router (Conexión a Internet)	Saturación de ancho de banda	Filtros de navegación	62.72
Impresora Multifuncional	Daño de equipo	Ventilación	0.3
Computador Portátil	Hurto de Maquina	Gualla	0

Omar Brito y Abel Sierra.

Informes – Este sector se dedica a la generación de informes para exponer los datos ingresados en la aplicación y también los resultados con base en ellos. La Figura 48 muestra la existencia de dos tipos de informe: el informe general y el informe por activo. De ambas existe la modalidad de visualización por browser y por descarga de un archivo PDF.

Figura 48. Generación de informes

Generar Informes

Tipo de Informe	ver	descargar
Informe General	Ver	Descargar
Informe por Activos	Ver	Descargar

Omar Brito y Abel Sierra.

Figura 49 muestra la primera modalidad de informe general, la cual consiste en exponer los valores crudos numéricos de la degradación, la probabilidad de ocurrencia, el impacto, el riesgo, y sus respectivos valores residuales, desde los cuales la aplicación se basa para realizar los resultados cualitativos que serán explicados más adelante. Finalmente, al principio de cada informe siempre habrá información del general del proyecto.

Figura 49. Informe general

Reporte Por Activo - 2017-10-02

Codigo	PROJ1
Organización	Constructora IACA y CIA Ltda http://www.constructoraiaca.com/
Propietario	Alberto Manuél Sierra
Versión	1.0

id	Nombre	Amenazas	Prob	Prob re	Deg	Deg re
7	Computador Portátil	Hurto de Maquina	0.1	0	1	0.2
8	Impresora Multifuncional	Daño de equipo	4	2	0.3	0.03
9	Router (Conexión a Internet)	Saturación de ancho de banda	20	14	0.8	0.56
12	Archivador	Acceso a archivos fisicos	2	0.2	0.25	0.025
10	Memoria USB	perdida	0.5	0	0.1	0.04
11	Disco Duro portátil	Cambios en los archivos	0.4	0	0.8	0.24

id	Nombre	Amenazas	Imp	Imp re	Ri	Ri re
7	Computador Portátil	Hurto de Maquina	9	1.8	0.9	0
8	Impresora Multifuncional	Daño de equipo	1.5	0.15	6	0.3
9	Router (Conexión a Internet)	Saturación de ancho de banda	6.4	4.48	128	62.72
12	Archivador	Acceso a archivos fisicos	2	0.2	4	0.04
10	Memoria USB	perdida	0.3	0.12	0.15	0
11	Disco Duro portátil	Cambios en los archivos	5.6	1.68	2.24	0

Omar Brito y Abel Sierra.

El informe por activos consiste en un reporte detallado de valores numéricos y valores cualitativos, cuya estructura es organizada por activos. Dichos valores cualitativos se basan en el criterio general propuesto por MAGERIT en el Libro II – Catálogo de Elementos, los cuales son el fundamento general para la generación de las tablas de calor. Cada tabla de calor es predeterminada (sus dimensiones consisten 5 filas por 5 columnas) y funciona como referencia para la exposición de la diferencia entre los resultados del impacto y el riesgo sin la aplicación de

salvaguardas y aquellos con la aplicación de salvaguardas, fácilmente visualizado por la convención de colores (azul para resultados sin salvaguardas, gris para resultados con salvaguardas). Un ejemplo de éste informe se encuentra en la Figura 50.

Es en este informe detallado que el usuario verá los resultados con claridad. La aplicación web hace ver la diferencia entre impactos y riesgos normales y residuales. El usuario será capaz de concluir con qué eficacia una salvaguarda logra mitigar la degradación y la probabilidad de ocurrencia de una amenaza sobre un activo, y si el usuario se siente en la obligación de hacer cambios sobre los valores calculados, la aplicación web estará en la capacidad de recibir valores nuevos o cambiados, lo cual conlleva a que el informe por activo demuestre el cambio en los resultados finales. Esto conlleva a que la aplicación provee dos conclusiones: o si existe mitigación de impacto y riesgo, o no, en el cual ambas convenciones de colores estarán en la misma posición dentro de las tablas de calor, siendo el color azul (sin salvaguarda) el que tiene prelación.

Figura 50. Informe por activo

Activo 2

Nombre:	Impresora Multifuncional
Amenaza	Daño de equipo
Valoración	Medio
Probabilidad	4
Degradación	0.3
Impacto	1.5
Riesgo	6
Salvaguarda	Ventilación
Probabilidad Residual	2
Degradación Residual:	0.03
Impacto Residual	10
Riesgo Residual	0.3

Impacto

	Degradación				
	0-20	**20-40**	**40-60**	**60-80**	**80-100**
Extremo	Alto	Muy Alto	Extremo	Extremo	Extremo
Muy Alto	Medio	Alto	Muy Alto	Extremo	Extremo
Alto	Bajo	Medio	Alto	Muy Alto	Extremo
Medio	Bajo	Bajo	Medio	Alto	Muy Alto
Bajo	Bajo	Bajo	Bajo	Medio	Alto

Riesgo

	Probabilidad				
	0-20	**20-40**	**40-60**	**60-80**	**80-100**
Extremo	Alto	Muy Alto	Extremo	Extremo	Extremo
Muy Alto	Medio	Alto	Muy Alto	Extremo	Extremo
Alto	Bajo	Medio	Alto	Muy Alto	Extremo
Medio	Bajo	Bajo	Medio	Alto	Muy Alto
Bajo	Bajo	Bajo	Bajo	Medio	Alto

Impacto y Riesgo Sin Salvaguarda

Impacto y Riesgo Con Salvaguarda

Omar Brito y Abel Sierra.

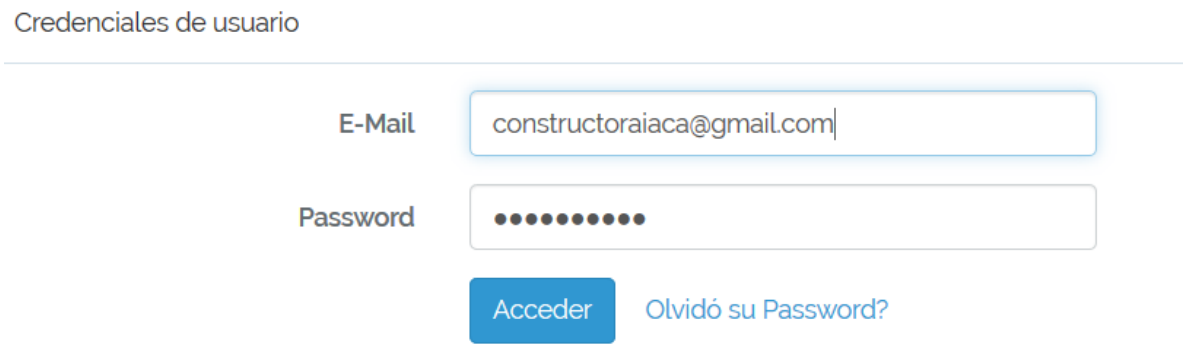
6. MANUAL DE USO

El propósito del presente documento es exponer un manual de uso de MAGERIT Free 1.0, una aplicación web de libre uso para el análisis y la gestión de riesgos de los sistemas de información según MAGERIT. Dado que en el capítulo anterior existe información acerca de la aplicación, sus componentes y su funcionamiento, el presente manual consiste en explicar funciones adicionales. Habrá nuevas imágenes y también referencias a imágenes colocadas en el capítulo anterior (en este caso, las imágenes no se repetirán en el manual) … Véase el numeral 5....

MAGERIT Free 1.0, como mencionado anteriormente, es una aplicación web de libre uso, dirigido a profesionales en el área de la seguridad de la información o informática, que desean emprender en el análisis y gestión de riesgos de los sistemas de información, que poseen conceptos fundamentales en la propuesta de MAGERIT para tal labor, y que necesitan una herramienta libre de costo e instalaciones que facilite el trabajo.

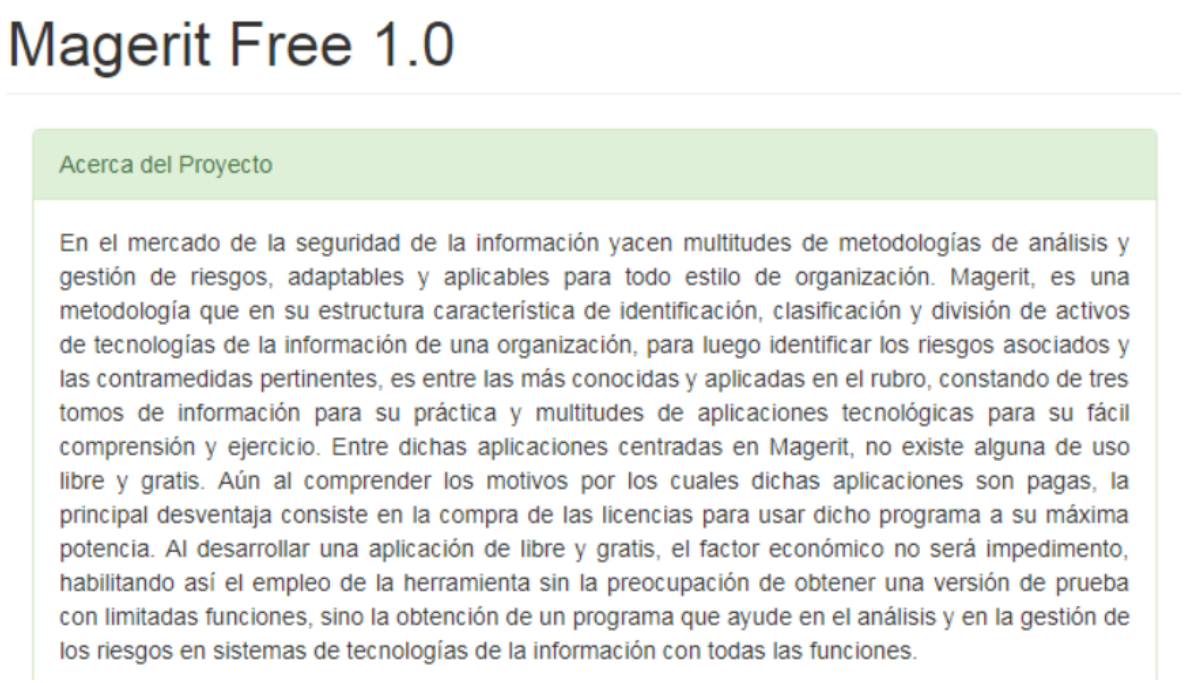
Primero, el usuario debe tener credenciales de ingreso a MAGERIT Free 1.0 (usuario/contraseña) para el ingreso a la aplicación. Este tiene la facultad de guardar el usuario y la contraseña para facilitar el ingreso a la aplicación en el futuro. Adicionalmente, desde el principio la aplicación da la bienvenida al usuario con un mensaje introductorio acerca de la justificación del desarrollo de MAGERIT Free 1.0. Figura 51 y Figura 52 presentan un ejemplo del acceso a MAGERIT Free 1.0.

Figura 51. Acceso a MAGERIT Free 1.0



Omar Brito y Abel Sierra.

Figura 52. Mensaje de inicio



Omar Brito y Abel Sierra.

Dicho mensaje se encuentra en el centro de la aplicación web, y a la izquierda se evidencia el menú principal, divido en tres secciones: Proyecto, Análisis de Riesgos e Informes. Cada sector cuenta con opciones que ayudan al propósito final por el cual MAGERIT Free 1.0 fue creado, cuyas funciones hacen parte de la propuesta original de MAGERIT. Cada opción o entidad provee algún medio por el cual el usuario será capaz de interactuar con MAGERIT Free 1.0 con facilidad, es decir, algunos cuentan con espacios de búsqueda, espacios para el ingreso de datos, y los siguientes botones básicos para la manipulación de información para la creación, edición, eliminación actualización, cálculo, almacenamiento y cancelación de datos, como visto en Figura 53.

Figura 53. Botones

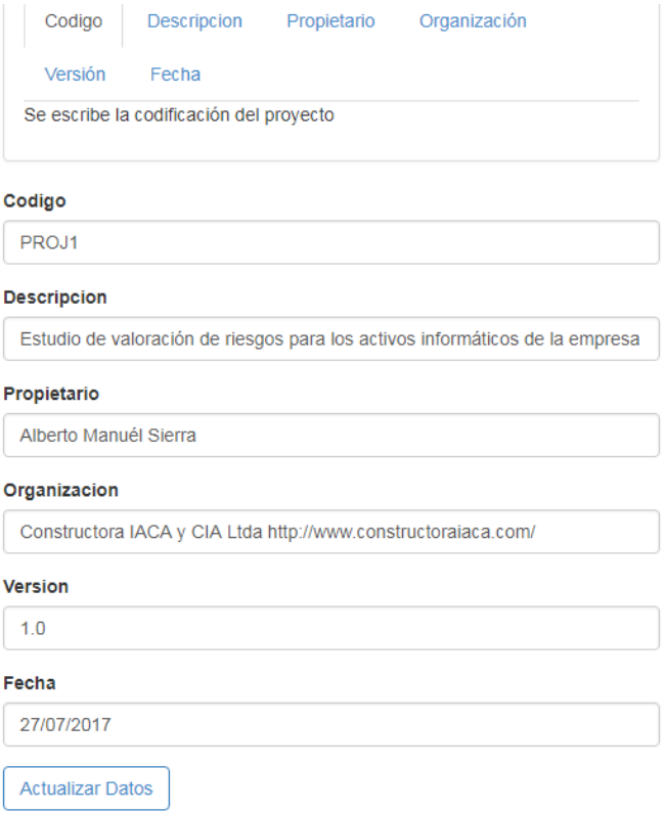
Omar Brito y Abel Sierra.

A continuación, se revela el uso y la función de entidad de MAGERIT Free 1.0.:

Proyecto – Esta entidad consta de sectores donde el usuario debe diligenciar los datos básicos de la creación del proyecto, crear los dominios de seguridad y donde el usuario halla referencias de los elementos relacionados con los criterios de valoración, dimensiones, activos, amenazas y salvaguardas.

Datos del Proyecto – Entidad donde el usuario diligencia los datos básicos de la creación del proyecto para el análisis y la gestión de riesgos de los sistemas de la información. Figura 54 presenta los atributos que deben ser diligenciados por el usuario.

Figura 54. Campos de datos de proyecto



Omar Brito y Abel Sierra.

Dominios de Seguridad - Entidad donde el usuario tiene la posibilidad de subdividir el proyecto en grupos de activos para proporcionar un enfoque en el análisis. Figura 55 revela los atributos que deben ser diligenciados por el usuario.

Figura 55. Campos de dominios

Omar Brito y Abel Sierra.

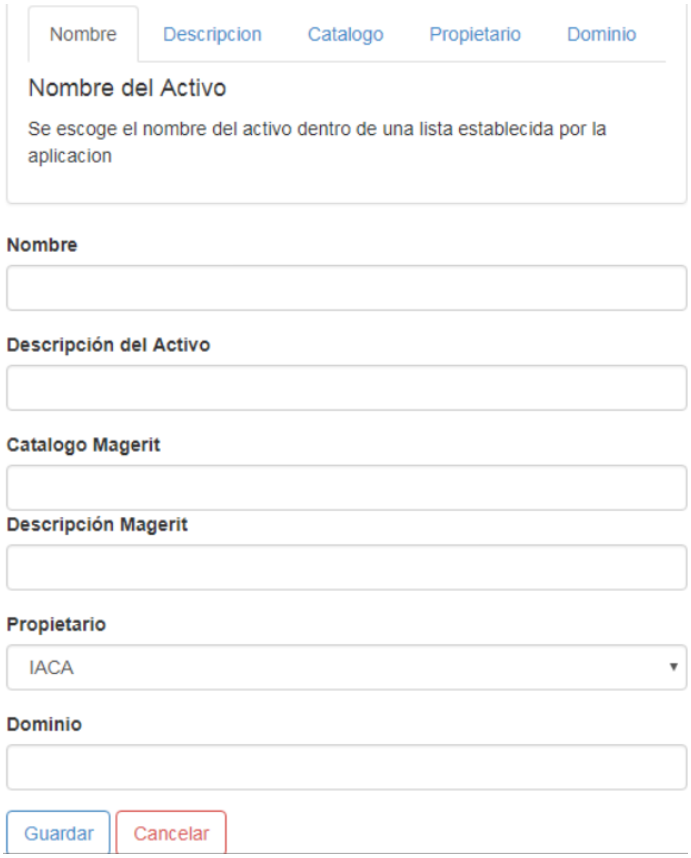
Catálogos – Luego sigue un subgrupo de entidades de catálogo de elementos, las cuales funcionan como entidades de referencia para la posterior selección de activos, amenazas y salvaguardas. Por su función, no existen campos que deben ser diligenciados por el usuario, sino que existe un espacio que es usado para la búsqueda de elementos. El usuario solo debe ingresar una palabra o porciones de una palabra y la aplicación filtra el elemento para ser revelado al usuario.

Análisis de Riesgos – Análisis de Riesgos es un sector destinado para la recepción de datos y para la generación de resultados. El usuario tendrá la oportunidad de ingresar datos, escoger elementos de catálogo, eliminar datos, y editarlos.

Activos, Amenazas y Salvaguardas - Estas entidades hacen uso de sus respectivos catálogos, por ejemplo, Catálogo de Activos para Activos, Catálogo de Amenazas para Amenazas y Catálogo de Salvaguardas para Salvaguardas. Los atributos son similares en las tres entidades y cada una cuenta con botones para agregar nuevos

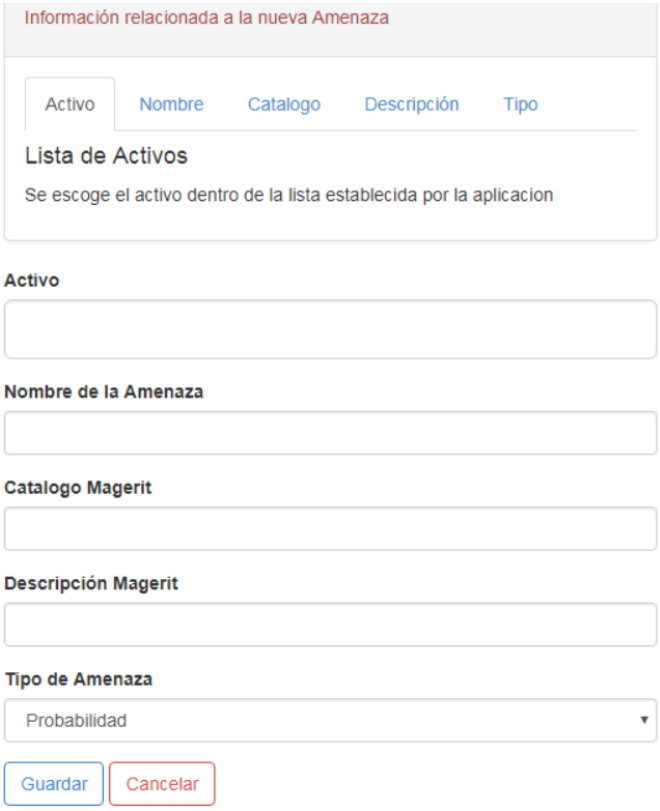
elementos, eliminarlos y para editarlos/actualizarlos. A continuación, presentamos los atributos en las imágenes Figura 56 y Figura 57, que deben ser diligenciados por el usuario.

Figura 56. Campos de activos



Omar Brito y Abel Sierra.

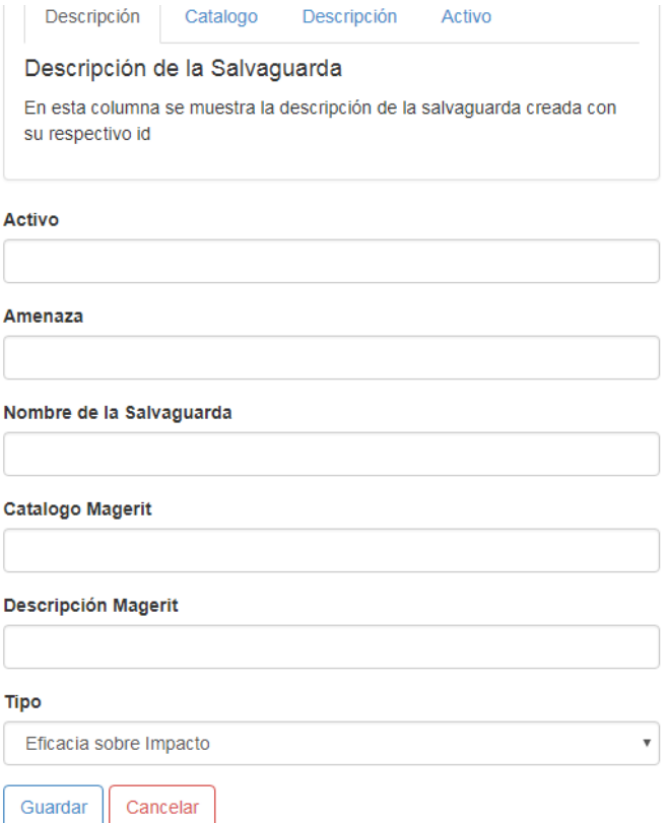
Figura 57. Campos de amenazas



Omar Brito y Abel Sierra.

Finalmente, la última entidad a diligenciar es ilustrada en la Figura 58.

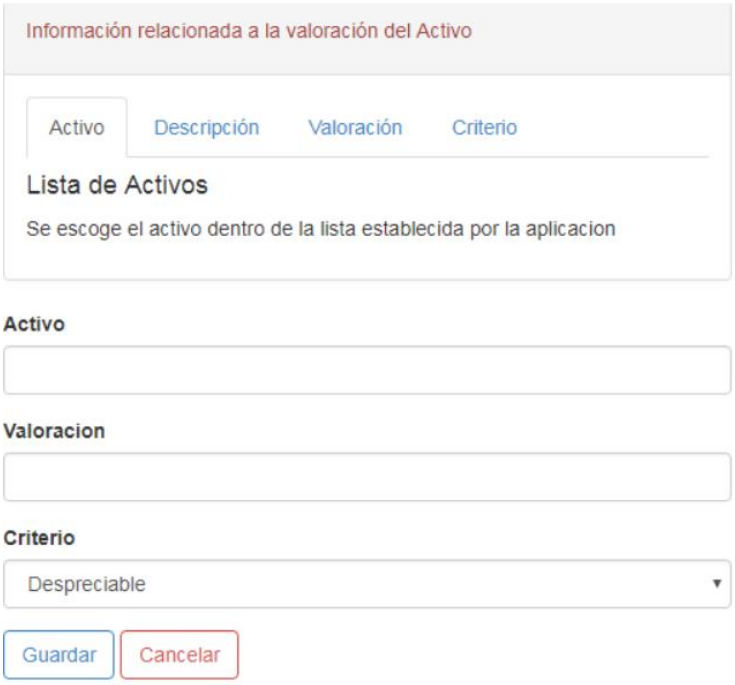
Figura 58. Campos de salvaguardas



Omar Brito y Abel Sierra.

Valoración – Esta entidad proporciona un espacio para ingresar el valor cualitativo del activo previamente escogido. Si el usuario ingresa el valor del activo en Valoración, MAGERIT Free 1.0. lo mapea a un valor cualitativo. Figura 59 presenta los campos importantes a diligenciar.

Figura 59. Campos de valoración



Omar Brito y Abel Sierra.

Degradación, Probabilidad, Eficacia/Impacto y Eficiencia/Probabilidad – Como mencionado anteriormente, estas entidades son destinadas para el ingreso de datos porcentuales y numéricos. En todos los casos, el usuario debe asociar cada dato a la amenaza o salvaguarda.

Impacto, Riesgo, Degradación Residual, Probabilidad Residual, Impacto Residual y Riesgo Residual - Finalmente, dentro del sector Análisis de Riesgo, la aplicación proporciona las entidades que ofrecen el cálculo automático de los valores ingresados en las entidades anteriores. Estas cuentan con un botón para realizar el cálculo entre los valores ingresados. Es decir, en estas entidades no cuentan con vistas de ingreso de datos ya que toman los datos recientemente ingresados y los usa para calcular un valor numérico, que luego será mapeado a un valor cualitativo en el resultado de los informes.

Informes – Este sector se dedica a la generación de informes para exponer los datos ingresados en la aplicación y también los resultados con base en ellos. Su menú es representado en la Figura 60. Existen de dos tipos de informe: el informe

general y el informe por activo. De ambas existen la modalidad de visualización por browser y por descarga de un archivo PDF, con botones llamados Ver o Descargar.

Figura 60. Menú de Informes

Omar Brito y Abel Sierra.

Informe General – Este estilo de informe consiste en exponer los valores numéricos crudos de la degradación, la probabilidad de ocurrencia, el impacto, el riesgo, y sus respectivos valores residuales, desde los cuales la aplicación se basa para realizar los resultados cualitativos. Finalmente, al principio de cada informe siempre habrá información del proyecto general.

Informe por Activo – Finalmente, este consiste en un reporte detallado de valores numéricos y valores cualitativos, cuya estructura es organizada por activos. Dichos valores cualitativos se basan en el criterio general propuesto por MAGERIT en el Libro II – Catálogo de Elementos, los cuales son el fundamento general para la generación de las tablas de calor. Como mencionado anteriormente, cada tabla de calor es predeterminada dimensiones de cinco por cinco y funciona como referencia para la exposición de la diferencia entre los resultados del impacto y el riesgo sin la aplicación de salvaguardas y aquellos con la aplicación de salvaguardas, que a su vez son resultados representados por convenciones de colores: azul para el primer resultado y gris para el segundo.

7. CONCLUSIONES

- Se logra crear una herramienta basada en la metodología MAGERIT de libre uso, basado en herramientas de libre uso como PHP y MySQL, de tal manera que el usuario final no esté forzado en pagar costos de compra de aplicación, licencias y honorarios.

- La interpretación de MAGERIT, las historias de uso y la obtención de datos reales (datos de la empresa Constructora IACA y CIA Ltda.) fueron los únicos requisitos necesarios previos usados para entender las características particulares que debe tener la aplicación web (por ejemplo, la descripción de terminología, el *login* del usuario, entre otras), los atributos de las entidades que conforman la base de datos y el funcionamiento general de la aplicación web en torno a la selección de activos.

- La elección de herramientas de libre uso (PHP, Laravel, MySQL, phpMyAdmin) para el desarrollo de la base de datos y la aplicación web resultaron eficaces para la sincronización de los datos almacenados con aquellos expuestos al usuario. No se incurrió en gastos para el uso de herramientas pagas, de licencias u honorarios.

- El uso de la metodología SCRUM, opuesto al uso de un proceso por cascada, permitió la constante comunicación entre los integrantes del grupo para entender el progreso en el que iba el proyecto y la constante retroalimentación de errores y correcciones sobre la aplicación, sin tener la obligación de rediseñar por completo procesos anteriores para mejorar resultados. Adicionalmente, dado que las historias de uso fueron plasmadas en el Backlog, éste registro funcionó como referencia para saber el estado actual en el que se encuentra el proyecto.

- El modelo Entidad-Relación resultante, que a su vez fue la fuente por la cual se desarrolló la base de datos, refleja cada elemento fundamental mencionado en el Libro III – Guía de Técnicas, y permitió el aporte de atributos necesarios para la interacción entre entidades, incluyendo la adición de un identificador de grupos de atributos diligenciados, que facilitó la obtención de resultados finales en la aplicación web, por ejemplo, la generación de los informes generales y por activos.

- Existe correcta sincronización entre la base de datos y la aplicación web en tiempo real, para ingresar datos, modificarlos, consultarlos, eliminarlos y calcularlos.

Esto fue comprobado al usar los datos reales provistos por la empresa Constructora IACA y CIA Ltda. Actualmente, la aplicación web es capaz de recibir nuevos datos y es capaz de editar aquellos previamente ingresados.

- Se generan exitosamente dos estilos de informe que exponen resultados tanto generales como detallados, por activo, junto con sus tablas de calor. Para futuras mejoras sobre la aplicación, existe aquella que consiste en la generación de informes basados en las amenazas y las salvaguardas, y en la libre propuesta de tablas de calor por parte del usuario, ya que aquellas implementadas son predeterminadas.

- MAGERIT es una propuesta práctica, amplia y densa, que permite su aplicación desde diferentes enfoques del análisis y gestión de riesgos y la presente aplicación web es un resultado de ello, donde el enfoque se concentra en dicho análisis por activos.

BIBLIOGRAFIA

APACHE FRIENDS. Xampp Apache+MariaDB+PHP+Perl. [en línea]- Disponible en: https://www.apachefriends.org/es/index.html

CN-CERT CENTRO CRIPTOLÓGICO NACIONAL. Ear/Pilar. [en línea], disponible en: https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar.html

--------. Ear/Pilar Entorno de Análisis de Riesgos. [en línea], disponible en: http://www.ar-tools.com/es/index.html

DESARROLLOWE6. ¿Qué es MVC?. [en línea]. Disponible en: https://desarrolloweb.com/articulos/que-es-mvc.html

ESEPE STUDIO ESPECIALISTAS 10.0. ¿Qué es MySQL?. [en línea]. Disponible en: http://www.esepestudio.com/noticias/que-es-mysql

GUAMANGA CHILITO, Carlos Arturo; PERILLA BUITRAGO, Carlos Leonardo. Análisis de Riesgos de Seguridad de la Información basado en la Metodología MAGERIT para el Área de Datacenter de una Entidad Promotora de Salud. Biblioteca Universidad Piloto de Colombia [PDF]. Bogotá D. C. 10 de diciembre de 2015. Disponible en la Biblioteca de la Universidad Piloto de Colombia

HANDY BACKUP. phpMyAdmin Definition. [en línea]. Disponible en: https://www.handybackup.net/backup_terms/phpmyadmin-definition.shtml

ISO 27000.ES. [en línea], disponible en: http://www.iso27000.es/glosario.html

LUCIDCHART. ¿Qué es un diagrama Entidad-Relación?. [en línea]. Disponible en: https://www.lucidchart.com/pages/es/qu%C3%A9-es-un-diagrama-entidad-relaci%C3%B3n

LYNDA. What is Laravel?. Laravel. [en línea]. Disponible en: https://www.lynda.com/Laravel-tutorials/What-Laravel/604257/648635-4.html

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS; MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. [en línea], disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

--------. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos. [en línea], disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

--------. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III – Guía de Técnicas. [en línea], disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

SAASMANÍA. Diferencia entre Plataforma y Aplicación. [en línea], disponible en: http://www.saasmania.com/blog/2008/04/10/diferencia-entre-plataforma-y-aplicacion/

TICBEAT. ¿Qué es el desarrollo ágil y cómo está transformando la industria del software?. [en línea]. Disponible en: http://www.ticbeat.com/tecnologias/que-es-el-desarrollo-agil-y-como-esta-transformando-la-industria-del-software/

VIDEO2BRAIN. Aprende SCRUM. [en línea]. Disponible en: https://www.handybackup.net/backup_terms/phpmyadmin-definition.shtml

WE LIVE SECURITY. MAGERIT: Metodología Práctica para Gestionar Riesgos. [en línea], disponible en: http://www.welivesecurity.com/la-es/2013/05/14/MAGERIT-metodologia-practica-para-gestionar-riesgos

ANEXOS

ANEXO A. Registro de reuniones SCRUM

Reuniones SCRUM		
Fechas	**Omar Brito**	**Abel Sierra**
14/07/2017	- La lectura de los libros de la metodología Mágerit. - Plasmar el Libro 3 en un diagrama de flujo simple. - Colaborar en el modelo Entidad-Relación trabajado por Abel.	- Redacción del Sprint con la pila de producto y las historias de usuario
22/07/2017	- Se complementó el Marco Teórico con los conceptos SCRUM, Modelo Entidad-Relación, Modelo-Vista-Controlador, entre otros. - Presentar el diagrama de flujo del Libro 3 de la metodología Mágerit, junto con una propuesta para la organización de la base de datos. - Crear una bitácora de las reuniones SCRUM del grupo de trabajo que seguirá siendo actualizada de aquí en adelante.	- Recolección de información básica para el marco teórico del documento del trabajo de grado. - Recolección de información acerca de la metodología SCRUM de desarrollos ágiles, para luego ser implementada en el desarrollo del trabajo de grado.
01/08/2017	- Redacción inicial del trabajo escrito. Su actualización y constantes mejoras entran a ser tareas y rutinas definidas.	- Desarrollo de la primera versión de la base de datos, cuyas entidades incluidas fueron Proyecto, Dominios, Dimensiones, Catálogos, Activos, Amenazas, Valoración, Salvaguardas, Impacto y Riesgo.
05/08/2017	- Pruebas de escritorio sobre la base de datos (tareas y rutinas definidas constantes sobre toda entrega de correcciones por parte de Abel). - Envío del resultado de las pruebas a Abel. Esto siempre será hecho luego de concluir con las pruebas de escritorio. - Adecuación del Marco Teórico del documento, incluyendo cambios en la pregunta-problema y objetivos. - Tareas y rutinas definidas.	- Corrección sobre las entidades previamente desarrolladas sobre la base de datos, por ejemplo, definición de unidades, campos de diligenciamiento de información, daños al cargar la base de datos, entre otras.

ANEXO A. (Continuación)

Reuniones SCRUM		
Fechas	**Omar Brito**	**Abel Sierra**
11/08/2017	- Adecuación de la estructura del trabajo de grado según el NTC 1486 (tareas y rutinas definidas). - Tareas y rutinas definidas.	Correcciones hechas sobre retroalimentación de Omar - Relacionar directamente el activo con su valoración. - Eliminar de la entidad Degradación los elementos Valoración_Código.
16/08/2017	- Consulta de bibliografías relacionadas con la aplicación de MAGERIT en empresas reales. - Creación de tablas de activos, amenazas y salvaguardas, en la cual se ingresarán los datos de la empresa real de escogencia. - Tareas y rutinas definidas.	Correcciones hechas sobre retroalimentación de Omar: - Quitar la valoración de Valoración. - Eliminar el atributo Tipo de la entidad Valoración - Quitar la entidad Dimensión_has_Amenaza. Adecuaciones generales sobre la base de datos.
21/08/2017	- Adecuación y reorganización de la pila de producto y de las historias de usuario en la aplicación donde se lleva el control de SCRUM (tareas y rutinas definidas). - Adecuación de los objetivos específicos, marco teórico y desarrollo de la base de datos (tareas y rutinas definidas). - Tareas y rutinas definidas.	Correcciones hechas sobre retroalimentación de Omar: - Inclusión de las entidades Degradación_Residual, Probabilidad_Residual, Impacto_Residual y Riesgo_Residual en el modelo Entidad Relación. - Inclusión de las mismas en la base de datos junto con sus atributos. - La entidad Degradación cambió a ser decimal en el backend. - En impacto falta escoger el ID de Degradación y de Valorización - En probabilidad le falta escoger el ID de Amenaza. - El valor del ARO dentro de la probabilidad debe ser un decimal. - Dentro de salvaguarda se quita la eficacia porque ya tenemos otras entidades llamadas Eficacia_sobre_Impacto y Eficacia_sobre_Probabilidad. Adecuaciones generales sobre la base de datos.
8/09/2017	- Tareas y rutinas definidas.	Desarrollo de la aplicación a nivel de frontend, en la cual se aplicaron las entidades Proyecto, Dominios, Dimensiones, Catálogos, Activos, Amenazas, Valoración y Salvaguarda

ANEXO A. (Continuación)

Reuniones SCRUM		
Fechas	**Omar Brito**	**Abel Sierra**
11/09/2017	- Actualización del trabajo escrito con nueva información e imágenes de la aplicación web. - Tareas y rutinas definidas.	Arreglos hechos sobre la aplicación: - Inclusión de información general de terminología en las entidades. - Inclusión de activos, amenazas y salvaguardas adicionales que faltaban en la base de datos original. Recopilación y organización de datos reales de Constructora IACA y CIA Ltda.
14/09/2017	- Tareas y rutinas definidas. - Inclusión de los datos de Constructora IACA y CIA Ltda. en el documento escrito, entre otras adecuaciones generales. - Inicio de la redacción del artículo IEEE del proyecto (tareas y rutinas definidas).	- Adecuación y restructuración total del modelo Entidad-Relación. - Inclusión del ID de la entidad Activos en todas las entidades de diligenciamiento de datos y de cálculo de datos.

ANEXO A. (Continuación)

Reuniones SCRUM		
Fechas	**Omar Brito**	**Abel Sierra**
21/09/2017	- Tareas y rutinas definidas. - Planteamiento de las tablas de calor para ser plasmados en la aplicación web y replanteamiento de fórmulas de entidades residuales.	Correcciones hechas sobre retroalimentación de Omar: - Poder ingresar libremente activos a demanda de usuario. - Eliminar el atributo Descripción de la entidad Valoración. - Quitar el signo "%" de la entidad Valoración. - Que la aplicación automáticamente asigne un criterio al valor de la Valoración. - Colocar las unidades en la entidad Probabilidad (frecuencia/año). - Cuando se escoja la degradación y/o la probabilidad, que el campo de amenaza ya este automáticamente relacionado con la entidad Amenaza. - Incluir la definición de la terminología en cada entidad de la aplicación web. - Incluir los códigos de las salvaguardas en la entidad Salvaguarda, según lo sugerido por MAGERIT. - Que después de escoger las eficacias, la aplicación web siempre devuelva al usuario a la entidad Salvaguardas. - Asociar la salvaguarda a la amenaza que mitigará. - Corregir el error de rutas que se presenta siempre que el usuario diligencia datos en las entidades y luego el usuario se devuelve al menú principal. - Cambiar el valor de probabilidad de entero a flotante. Adecuaciones generales en la aplicación web.
25/09/2017	- Tareas y rutinas definidas. - Presentación de propuesta de informe y tablas de calor.	Correcciones hechas sobre la retroalimentación de Omar: - Corregir las fórmulas de las entidades que calculan valores residuales. - Corregir los resultados generales ya que los valores estaban siendo calculados por estimación y no por exactitud decimal. Adecuaciones generales en la base de datos y en la aplicación web.
26/09/2017	- Tareas y rutinas definidas.	- Desarrollo de informes generales y por activos. - Inclusión de tablas de calor como referencias de Impacto y de Riesgos.

ANEXO A. (Continuación)

Reuniones SCRUM		
Fechas	**Omar Brito**	**Abel Sierra**
30/09/2017	- Tareas y rutinas definidas.	Correcciones hechas sobre la retroalimentación de Omar: - Asignar el criterio automáticamente luego de ingresar el valor de la valoración - Colocar las referencias porcentuales en la barra deslizadora de las entidades Degradación, Degradación_Residual, Probabilidad_Residual. - Evitar la desaparición de las tablas de resultados en las entidades pertinentes. - Que la aplicación calcule valores exactos y no redondeados. - Colocar el signo porcentaje en la tabla de impacto sin salvaguarda y con salvaguarda. - Colocar ocurrencias/año como unidades de probabilidades. Adecuaciones generales sobre la aplicación.
5/10/2017	- Tareas y rutinas definidas.	Ajustes finales en los informes: - Síntesis de tablas de calor. - Mapeo de valores crudos en los criterios de la valorización.

Omar Brito y Abel Sierra.